LAUREA AMMATTIKORKEAKOULU Uuden edellä

Tietoturvallisuustilanteen kartoitustyökalu pienille yrityksille

Kurittu, Veli Antti

2014 Leppävaara

Laurea-ammattikorkeakoulu
Leppävaara

Tietoturvallisuustilanteen kartoitustyökalu pienille yrityksille

Veli Antti Kurittu
Turvallisuusalan koulutusohjelma
Opinnäytetyö
Maaliskuu, 2014

Laurea-ammattikorkeakoulu **Tiivistelmä**
Leppävaara
Turvallisuusalan koulutusohjelma

Veli Antti Kurittu

Tietoturvallisuustilanteen kartoitustyökalu pienille yrityksille.

Vuosi 2014 Sivumäärä 65

Tässä toiminnallisessa opinnäytetyössä kuvaillaan prosessi, jonka tuloksena syntyi Tikka-niminen työkalu pienten yritysten tietoturvallisuusriskien kartoitukseen. Se on suunnattu yrityksille, joissa tietoturvallisuustyötä ei joko ole tehty tai jossa se on vasta aloitettu. Työtä varten tehdyssä, rikostorjunnan ammattilaisille suunnatussa kyselyhaastattelussa ja kirjallisuuskatsauksessa tunnistettiin, että keskeinen ongelma tietoturvallisuuden ongelmiin yrityksissä on sekä tietämättömyys tietoturvallisuusasioista että tietoturvallisuuden laiminlyönti. Työkalu esittelee kuuden fiktiivisen, todellisiin esimerkkeihin yksityiskohdiltaan perustuva tarinan perusteella erilaisia tapahtumia, joissa tietoturvallisuusriski on realisoitunut ja johtanut haitallisiin seurauksiin. Tällä tavoin työkalu tuo tietoturvallisuusriskit lähelle arkielämää ja auttaa käyttäjäänsä hahmottamaan, mistä tietoturvallisuudessa oikeastaan on kysymys.

Asiasanat: tietoturvallisuus, riskienhallinta, yritystoiminta

Laurea University of Applied Sciences **Abstract**
Laurea Leppävaara
Bachelor's Degree Programme in Security Management

Veli Antti Kurittu

Information security risk assessment tool for small businesses.

Year 2014 Pages 65

This functional bachelor's thesis describes a process, which culminated in the creation of a tool that is used for information security risk assessment in small businesses. The tool is a point-of-entry, first contact resource for matters concerning information security for entrepreneurs who have not previously carried out any work on information security matters or are only beginning the process of information security management. A questionnaire aimed at law enforcement computer crime professionals was used to gather information about the most common risks involved in small business information security practices and policies. The tool uses six different fictional stories that have details from actual events to showcase different scenarios of information security incidents with real-world negative effects. By doing this, the tool brings the subject of information security into a real-world context and helps the user of the tool to understand the nature and significance of information security.

Keywords: information security, risk management, business

Sisällys

1 Johdanto

Tässä toiminnallisessa opinnäytetyössä etsitään kirjallisuuskatsauksen ja asiantuntijakyselyn avulla pienten yritysten merkittävimpiä tietoturvauhkia. Keskeisten, yrityksiä uhkaavien tietoturvariskien tunnistamisen perusteella laaditaan case-kuvauksiin perustuva tarinapohjainen työkalu, jonka avulla yrittäjät voivat kasvattaa omaa ymmärrystään tietoturvallisuudesta.

1.1 Työn tausta ja tutkimuskysymys

Idea työn aiheeseen syntyi entisessä työssäni tietotekniikkarikostutkijana Helsingin rikospoliisissa. Työssäni kohtasin jatkuvasti pieniä yrityksiä, jotka olivat joutuneet tietoturvarikosten uhreiksi. Huomasin nopeasti, että yhteinen nimittäjä kaikille näille tapauksille oli se, että yritysten tietoturvallisuuden perusasiat oli laiminlyöty. Tämä johtui pääsääntöisesti siitä, että yritysten johdolla ei ollut tietoa tai ymmärrystä siitä, miten merkityksellinen asia tietoturvallisuus yritystoiminnassa on. Yritykset olivat keskittyneet omaan toimintaansa, ja tietotekniikkaa oli hankittu ja alettu käyttämään ajattelematta tiedonkäsittelyyn liittyviä turvallisuusnäkökulmia laisinkaan. Tietoturvallisuutta ei selkeästi mielletty yritystoiminnan olennaiseksi osa-alueeksi eikä siihen liittyviä riskejä otettu yritystoiminnassa juuri mitenkään huomioon. Riskeistä ei edes oikeastaan oltu tietoisia, ja jos oltiin, kuviteltiin, ettei omassa toiminnassa syystä tai toisesta tarvitse näitä riskejä hallita. Tämä altisti yritykset sekä tietoverkkorikoksille että heikensi yritysten kykyä toipua tietoturvallisuutta uhkaavista laiterikoista ja muista, sisäisistä häiriöistä.

Monet yritykset ryhtyivät miettimään ja korjaamaan tietoturvakäytäntöjään vasta sen jälkeen, kun olivat joutuneet tietoturvaloukkauksen uhreiksi. Tällöin vahingot olivat kuitenkin jo syntyneet. Ajatuksissani oli, että tietoturvallisuustyön aloittaminen nimenomaan pienissä yrityksissä pitää tehdä helposti ymmärrettäväksi siten, että kuka tahansa yrittäjä joka työskentelee tietoteknisten laitteiden kanssa voi päästä tietoturvallisuustyössä alkuun. Työkalu kohdistettiin pienille yrityksille nimenomaan siksi, että suurissa yrityksissä voidaan olettaa olevan jo tietohallinnollista osaamista sen verran, että tietoturvallisuuden perusasiat on otettu toiminnassa huomioon.

Tämän opinnäytetyön keskeinen tutkimuskysymys on seuraava:

Mitkä keskeiset, virheelliset käytännöt tai politiikat altistavat pieniä yrityksiä tietoturvaloukkauksille ja -häiriöille?

Tutkimuskysymys on aseteltu siten, että se kattaa laajan skaalan eri tietoturvallisuuden tasoille ja osa-alueille asettuvia vastauksia. Käytännöillä tarkoitetaan yrityksissä tapahtuvia,

konkreettisia toimintatapoja jotka liittyvät turvattavan tiedon käsittelyyn. Politiikoilla käsitellään yritysten ohjeistettuja käytänteitä joiden väärä sisältö tai puutteellisuus aiheuttaa tietoturvariskejä. Kysymys kattaa sen, miten riskienhallintaa on pyritty ohjaamaan ja miten todellisuudessa toimitaan.

Työssä käytetään tiedonkeruumenetelminä kirjallisuuskatsausta sekä laadullisen tutkimuksen menetelmiä. Menetelmiä käytetään sekä kyselylomakkeen muodossa että työkalun koekäyttäjien lomakehaastatteluna. Kyselylomakkeella saatavien tietojen analysointitapana käytetään teemoittelua. Työkalun koekäyttäjien kokemuksia referoidaan työkalun testauksen analysointivaiheessa.

Tässä työssä ei tarjota valmiita malleja pienten yritysten tietoturvallisuuden hallintaan, sillä yksittäisten yritysten tarvitsemat ratkaisut ovat yksilöllisiä ja riippuvat niiden käsittelemät tiedon laadusta, luonteesta ja määrästä. Myös toimintaympäristö luo omat puitteensa sille, miten tietoturvallisuuden yksityiskohdat toteutetaan. Alan standardit ja mallit voivat olla hyvin raskaita ja vaikeasti lähestyttäviä, joten niistä aloittaminen on helposti ylitsepääsemättömän vaikeaa. Yleiset, hyvän tietoturvatoiminnan pohjalla olevat aihekokonaisuudet ovat kuitenkin yleisluontoisia ja ne pätevät lähes kaikkeen yritystoimintaan (Miettinen 1999, 15).

1.2 Keskeiset käsitteet

Pieni yritys tarkoittaa yritystä, jolla on alle 50 työntekijää ja jonka vuosiliikevaihto on enintään 10 miljoonaa euroa tai jonka taseen loppusumma on enintään 10 miljoonaa euroa. Näiden kriteerien lisäksi pienen yrityksen tulee täyttää Tilastokeskuksen määritelmän riippumattomuudesta. Riippumattomuus yritystoiminnassa edellyttää, että yrityksen pääomasta tai äänivaltaisista osakkeista 25 prosenttia tai enemmän ei ole yhden tai useamman yrityksen omistuksessa, joihin ei voida soveltaa pienen tai keskisuuren yrityksen määritelmää. (Tilastokeskus 2013.)

Riski tarkoittaa mahdollista tapahtumaa ja sen seurauksia. Riskin käsitteeseen liittyy riskienhallinta, jolla tarkoitetaan riskien tunnistamista, analysointia ja arviointia. Riskienhallinnan tarkoituksena on välttää toteutuneista riskeistä seuraavat tapahtumat ja niiden haitalliset vaikutukset toimintaympäristöön. Riskienhallintatyötä tehdään poistamalla riskin syy, muuttamalla riskin toteutumisen todennäköisyyttä tai muuttamalla riskin toteutumisesta aiheutuvia vaikutuksia. (ISO 31000:2013, 12.)

Tietoturvallisuus on määritelty usealla, toisistaan joltain osin poikkeavalla tavalla kirjallisuudessa ja erilaisissa standardeissa. Käsitteestä ei ole yksittäistä, keskeistä ja kaikenkattavaa määritelmää. Tietoturvallisuutta käsitellään tässä työssä osana organisaatioiden toimintaa, joten se voidaan määritellä tätä kautta. Organisaatioiden pääomana oleva tieto halutaan pi-

tää luotettavana, nopeasti saatavana, oikeassa muodossa ja ainoastaan oikeiden henkilöiden saatavilla. Tietoturvallisuuden voi näiden tavoitteiden kautta tiivistää kolmeen keskeiseen tiedon ominaisuuteen – tiedon luottamuksellisuuteen, tiedon käytettävyyteen ja tiedon eheyteen. Tätä kutsutaan myös klassiseksi, tiedon arvoon perustuvaksi määritelmäksi. Käsitettä on laajennettu tietoyhteiskunnan murrosvaiheessa kattamaan sähköisiä tietojärjestelmiä koskevia käsitteitä, joita ovat yllä mainitun kolmen ominaisuuden lisäksi *kiistämättömyys* ja *pääsynvalvonta*. (Hakala ym. 2006, 4-5.)

2 Toiminnallinen opinnäytetyö

Toiminnallinen opinnäytetyö on opinnäytetyön tekemisen tapa, jonka tuloksena syntyy tosielämän toiminnassa käytettävä ohjeistus, opas tai toimintaa parantava tuotos. Toiminnallisen opinnäytetyön olennainen ero perinteiseen opinnäytetyöhön on se, että toiminnallinen opinnäytetyö ei ole tutkimus. Toiminnallisessa opinnäytetyössä voidaan käyttää, ja usein käytetäänkin, tutkimuksellisia menetelmiä, mutta niiden tuloksena syntyvä työ ei itsessään täytä tutkimuksen määritelmää. Toiminnalliseen opinnäytetyöhön kuuluu siinä käytettyjen, tutkimuksellisten menetelmien kuvaus. Menetelmissä pitäydytään usein humanististen tieteiden perusmenetelmissä. Menetelmiä käytetään ensisijaisesti tiedonkeruuseen, jonka pohjalta toiminnallisen opinnäytetyön tavoitteena oleva työ tehdään. (Vilkka & Airaksinen 2003, 9.)

Ammattikorkeakouluopetuksen tavoitteena on, että oppilaalla on valmistumisensa jälkeen mahdollisimman hyvät mahdollisuudet työllistyä alansa asiantuntijatehtäviin. Näissä tehtävissä tarvitaan kehittämisen ja tutkimuksen perusteiden tuntemusta, joten opinnäytetyönkin pitää heijastaa tätä osaamista. Toiminnallinen opinnäytetyö antaa mahdollisuuden käyttää tutkimuksellisia menetelmiä ja tuottaa niiden perusteella esimerkiksi opas, portfolio, kotisivut tai vaikka tapahtuma. (Vilkka & Airaksinen 2003, 10.)

Toiminnallisessa opinnäytetyössä käytettävät laadulliset ja määrälliset menetelmät voivat toimia opinnäytetyön pohjana käytettävän tiedon lähteinä. Kerättyä tutkimusaineistoa ei välttämättä tarvitse analysoida sen tarkemmin, vaan sitä voi käyttää samoin kuin muita lähteitä. Jos analysoinnilla halutaan saada tutkimustietoa sisällöllisten valintojen perusteluun, voi aineiston analysoinniksi riittää esimerkiksi tyypittely tai teemoittelu. (Vilkka & Airaksinen 2003, 56-58.)

2.1 Kirjallisuuskatsaus

Kirjallisuuskatsaus on menetelmänä olennaisen, aikaisemman tutkimuksen arviointia ja läpikäymistä. Sen avulla esitellään lukijalle aikaisempi aiheesta tai aihepiiristä tehty tutkimus ja siihen liittyvä käsitteistö sekä tutkimusongelmat jotta uuden tutkimuksen merkitystä aikaisempaan on mahdollista arvioida. Kirjallisuuskatsaus toimii myös oman tutkimuksenteon apu-

välineenä ja se on välttämätön osa oman tutkimuksen perustelua ja näkökulman valitsemista. (Turun yliopisto, 2014.)

Kirjallisuuskatsaus keskittyy tutkimusongelman kannalta keskeiseen lähdemateriaaliin ja kirjallisuuteen, kuten aikakauslehtiin, tutkimusselosteisiin ja muihin keskeisiin julkaisuihin. Kirjallisuuskatsauksessa on pyrittävä arvioimaan lukijalle merkitykselliset keskeiset näkökulmat, tärkeimmät tutkimustulokset ja johtavat tutkijanimet. Kirjallisuuskatsauksen kautta tutkimustyö asettuu osaksi aihepiiristä tehtyjen tutkimusten kokonaisuutta. Kirjallisuuskatsauksessa on arvioitava mahdollisesti eriäviä näkökulmia ja suhtauduttava niihin kriittisesti. Myös esille tulevat näkemyserot on tuotava kirjallisuuskatsauksessa esille. Kirjallisuuskatsaus edellyttää aiheen tuntemusta siltä osin, että katsauksen tekijän on osattava valita katsaukseen vain asianmukainen ja suoraan tutkimusongelmaan liittyvä kirjallisuus. Kirjallisuuskatsaus tarjoaa opiskelijalle myös erinomaisen mahdollisuuden uuden oppimiseen. (Hirsjärvi ym. 2005, 111-113.)

Tutkijan ei kuitenkaan tule erotella ja esitellä kaikkea omaan tutkimusongelmaansa liittyvää kirjallisuutta tasapuolisesti, vaan poimia objektiivisten ja tasapuolisten arvioiden perusteella kirjallisuudesta olennainen osuus oman tutkimuksensa tueksi. Näkökulmat on syytä erotella siten, että erilaiset näkökulmat erottuvat selkeästi toisistaan. (Hirsjärvi ym. 2005, 111-113.)

2.2 Tarinankerronta tiedonvälitystapana

Tarinankerronta on ihmiselle ominainen tapa siirtää ja jakaa tietoa. Ihmiskunnan suullisen tarinankerronnan perinne on syntynyt kauan ennen kirjoitus- ja painotaidon keksimistä ja se on ollut keskeinen kulttuuriperimän välityksen väylä mahdollisesti satojen tuhansien vuosien ajan. Ihmiset kertovat toisilleen tarinoita inspiroidakseen toisiaan ja välittääkseen tietoa, arvoja ja asenteita sekä vahvistaakseen yhteisön sisäisiä siteitä. Tarinankerronnan voima tiedonvälityksen kanavana stimuloi ihmisen tunteita ja kohdistaa niitä kohti yhtä tavoitetta. Tarinoissa tapahtuu myötäelämistä. Monet pitävät nykyään taitoa kertoa tarinoita edellytyksenä hyvälle johtajuudelle. Tarinoiden kertomisen trendi ottaa huomioon ihmisten tarpeen saada asiatietoa viihdyttävässä muodossa mielenkiinnon ylläpitämiseksi. (Plain Language at Work 2012)

Tarinan määrittelylle on useita vaihtoehtoja. Eräs määritelmä on ”kaksi tai useampi väitettä, jotka on järjestetty ajalliseen järjestykseen.” Tässä merkityksessään tarina opettaa tietoa rakentamalla tapahtumista kuulijan tai lukijan mielessä johdonmukaisen tapahtumaketjun, jossa syy-seuraussuhteet seuraavat loogisesti toisiaan. Tarinan kielelliset ja ajalliset rakenteet toimivat tarinan vastaanottajan huomiota suuntaavina tekijöinä. Erityisenä huomionsuuntaamismenetelmänä toimii tarinan kokonaisuutta läpäisevä juoni. Tarinan tarkoitus voi

olla joko opettava, viihdyttävä tai näitä yhdistävä. Kaikille tarinan muodoille yhteisenä tekijänä on tarinan kokemuksellinen olemus erotuksena muunlaisen tiedonvälityksen, kuten taulukoiden, kaavioiden tai faktojen listaamisen abstraktista luonteesta. Tarinan muotoon rakennetut opetuksen muodot voidaan jakaa niiden toteutuksen mukaan neljään eri kategoriaan: case-kuvauksiin, skenaariotarinoihin, narratiiveihin ja ongelmakeskeisiin opetuskokonaisuuksiin. (Andrews ym. 2009, 7-8)

Case-kuvauksille keskeistä on se, että tarinan lopputulema on selvillä. Tarina kertoo tapahtumat niiden alkutilanteesta loppuratkaisuun. Oppija tarkastelee case-tapausta ulkopuolelta ja suhtautuu siihen jo tapahtuneiden asioiden kuvauksena. Case-tutkimus herättää kuulijassa usein paljon kysymyksiä ja caseen liittyvä tarina tarjoaa samaistumisen kohteen. Kuulija vertailee tarinan tapahtumia ja lähtökohtia itse kokemiinsa asioihin, ja usein tästä syntyy voimakas vuorovaikutustilanne, varsinkin mikäli case-tarina kerrotaan suoraan suullisesti yleisölle. (Andrews ym. 2009, 7-8.)

Tyypillisesti yleisölle herää vaihtoehtoisia ratkaisumalleja casessa toteutettuihin malleihin ja ehdotuksia sekä tarve kysyä neuvoa vastaaviin tapahtumiin, joita kuulijalle itselleen on tapahtunut. Tässä ilmenee se, että kertomuksellinen tiedonvälitystapa luo kertojan ja kuuntelijoiden välille hyvän vuorovaikutussuhteen ja tarinassa kerrotut tapahtumat ovat aiheuttaneet samaistumisen tunteita kuulijassa. (Doty 2003.)

2.3 Asiantuntijakysely

Kyselylomake on tiedonkeruun tutkimuksellinen menetelmä. Kyselylomakkeen ulkoasuun ja laajuuteen pitää kiinnittää huomiota. Lomakkeen jakaminen osioihin ja palstoittaminen säästää tilaa ja tekee lomakkeesta selkeästi hahmotettavan. Lomakkeen on hyvä edetä ylhäältä alaspäin, ja jos tästä poiketaan, on lomaketta hyvä hahmottaa sen täyttäjälle käyttämällä esimerkiksi nuolia tai muita visuaalisia ohjeita. Lomakkeeseen vastaamisen suositeltu enimmäisaika on noin 15-20 minuuttia, joten liian pitkä tai sekava lomake saattaa aiheuttaa tilanteen, jossa hyvinkin suunniteltu kysely saa vähän vastauksia. Lomakkeiden kysymyksensuunnittelun tulee olla sellaista, että vastaajat ymmärtävät kysymykset samalla tavalla ja vastaavat niihin yhteismitallisesti. Tämä vahvistaa lomakkeella saatujen vastausten vertailukelpoisuutta. Kysymysten on oltava myös helposti ymmärrettäviä väärinkäsityksistä johtuvien vastauserojen minimoimiseksi. (KvantiMOTV 2011.)

Lomakkeen laadinnassa on kiinnitettävä huomiota ulkoasun lisäksi sisällön loogisuuteen. Samaa aihepiiriä käsittelevät kysymykset on koottava yhteen, vaikka lomake sinänsä saakin sisältää useasta eri aihepiiristä olevia kysymyksiä. Looginen, selkeä rakenne helpottaa lomakkeen täyttämistä. Kyselyn kieliasu määräytyy kyselyn tekijän ja vastaajan keskinäisten suh-

teiden mukaan. Lomakkeessa on hyvä käyttää teitittelyä, mutta myös sinuttelu tulee kyseeseen mikäli vastaajien ja kyselyn tekijän välit ovat tuttavalliset. Sopivan tavan valinta riippuu kyselyn kohderyhmästä. Taustatietoja, kuten ikää, sukupuolta tai esimerkiksi tuloja kerättäessä on hyvä ilmoittaa, että tiedot kerätään vain tilastollista analyysia varten. (KvantiMOTV 2011.)

Kyselyn sisällön osalta on pyrittävä kysymyksiin, joihin saadaan mahdollisimman tarkkoja vastauksia. Hienojakoista vastausmateriaalia on helppo tiivistää, mutta suurella ja karkealla hajonnalla olevia tuloksia ei saa kyselyn tekemisen jälkeen enää jaoteltua pienempiin osiin. Pääsääntöisesti on hyvä idea käyttää strukturoituja kysymyksiä, eli kysymyksiä joihin tarjotaan valmiit vastausvaihtoehdot. Avoimia kysymyksiä käytettäessä pitää harkita tarkoin, miksi päädytään nimenomaan avoimeen kysymykseen, ja voisiko kysymyksen esittää strukturoidussa muodossa. Monissa laajoissa kyselyissä avoimet kysymykset saattavat jäädä täysin vaille vastausta. Kuitenkin mikäli kysymyslomakkeen täyttäjäjoukko tiedetään aktiiviseksi ja helposti kirjallisesti kantaa ottavaksi, voidaan avointen kysymysten käyttöä pitää hyvinkin perusteltuna. (KvantiMOTV 2011.)

Sanallisissa vastauksissa voidaan käyttää mittausmenetelmiä, joissa eri vastauksille annetaan numeerinen arvo. Tällaisia järjestysasteikkoja ovat mm. Likertin asteikko, jossa vastausvaihtoehdot pisteytetään viisijakoisesti asteikolle ”Täysin eri mieltä – täysin samaa mieltä”. Käytännössä sanallisten asteikkojen käyttäminen voi olla hankalaa, sillä erilaisilla sanallisilla, numeroiduilla vastauksilla voi olla ihmisille erilaisia merkityksiä. Pääsääntöisesti sanalliset muuttujat koodataan analysointivaiheessa numeroilla matriisiin, jolloin vastauksille voidaan tehdä laskutoimituksia kuten keskiarvolaskentaa. (KvantiMOTV 2007.)

2.4 Vastausten teemoittelu

Kyselytutkimuksen avointen tekstivastausten teemoittelu on analysointimenetelmä, jossa kyselyllä kertyneestä aineistosta etsitään niitä yhdistäviä tai erottavia tekijöitä. Teemoittelu on luonteva etenemistapa haastatteluaineiston analysoimisessa. Aineisto voidaan järjestellä teemoittain esimerkiksi leikkaamalla ja liimaamalla eri teemojen alle sopivia vastauksia ja keräämällä tällä tavoin materiaalia eri teemojen alle. Aineiston järjestely tällä tavoin voidaan hoitaa esimerkiksi teemakortiston avulla leikkaamalla tulostetusta aineistosta kaikki teemaan liittyvät kohdat ja keräämällä ne omiksi kokonaisuuksikseen. Saman voi nykyään tehdä myös tekstinkäsittelyohjelman avulla leikkaa-liimaa – toimintoja soveltamalla. Tutkimusaineiston teemoja käsiteltäessä voidaan käyttää teemoja kuvaavia näytepaloja eli sitaatteja, joiden tehtävänä on osoittaa, että teema on tosiasiassa johdettu nimenomaan saadusta aineistosta. Sitaattien käyttämisessä on kuitenkin oltava kriittinen ja raporttia kirjoitettaessa

on hyvä miettä, onko sitaatti tarpeellinen. Teemoittelevat tutkimusraportti ei saa olla vain sitaattikokoelma vaan aineistoa pitää analysoida. (Saaranen-Kauppinen & Puusniekka 2006.)

Teemoittelun tavoitteena on nostaa esiin tutkimusongelmaa valaisevia teemoja, eli aineistosta pyritään nostamaan esiin nimenomaan tutkimusongelman kannalta olennaiset aiheet. Kyse on saadun materiaalin pelkistämisestä. Teemoittelu soveltuu ratkaisutavaksi silloin, kun tavoitteena on käytännön ongelman raktaiseminen. (Silius 2008, 4.)

3 Yrityksen tietoturvallisuus

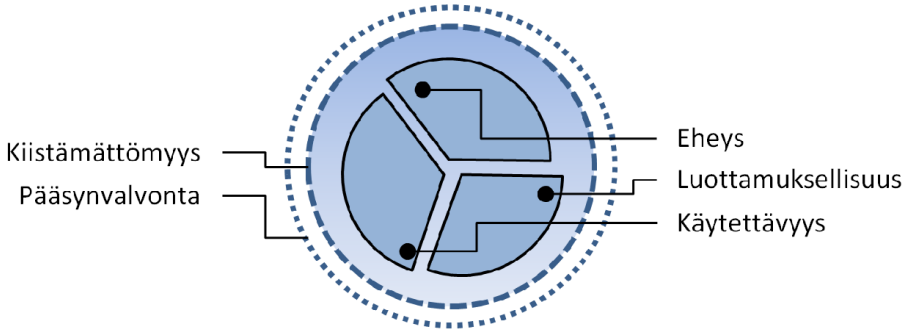
Tietoturvallisuus on yleisesti määritelty viiteen osa-alueeseen, joista tiedon luottamuksellisuus, käytettävyys ja eheys kuuluvat tiedon arvoon perustuvaan, klassiseen määritelmään. Tätä määritelmää on laajennettu koskemaan myös tietojärjestelmiä, ja sitä on laajennettu käsitteillä kiistämättömyydestä ja pääsynvalvonnasta.

3.1 Tietoturvallisuus käsitteenä

Tietoturvallisuuden käsitettä voidaan lähestyä sen osa-alueiden kautta, jotka ovat tiedon eri ulottuvuuksia. Tietoturvallisuuden käsitteen piiriin kuuluvat järjestelyt, joilla pyritään varmistamaan tiedon käytettävyys, eheys ja luottamuksellisuus (Valtionvarainministeriö 2008). Tiedon luottamuksellisuus (eng. confidentiality) tarkoittaa sitä, että tietojärjestelmiin tallennettuun tietoon pääsy on suojattu ulkopuolisilta ja tieto on rajattu vain niiden tahojen saatavaksi, joille se on tarkoitettu. Tiedon käytettävyys (eng. availability) merkitsee sitä, että tiedot ovat tietojärjestelmässä saatavilla nopeasti ja oikeassa muodossa. Tiedon eheys (eng. integrity) taas tarkoittaa sitä, etteivät käsiteltävät tiedot muutu ei-tarkoituksenmukaisesti tai pidä sisällään virheitä. (Hakala ym. 2006, 4)

Tietoturvallisuuden laajennettuun määritelmään kuuluvat myös kiistämättömyyden ja pääsynvalvonnan käsitteet. Tietojärjestelmät pyritään pitämään ainoastaan sen käyttäjäjoukon käytettävissä joille järjestelmä on tarkoitettu ja sulkemaan ulkopuoliset pois järjestelmästä joko järjestelmän resurssien säästämiseksi ja tiedon itsensä suojaamiseksi. Kiistämättömyydellä (eng. non-repudiation) tarkoitetaan tietojärjestelmän kykyä tunnistaa tietoa tallentava henkilö ja tallentaa tiedon lisäksi *metatietoa* siitä, kuka tiedon on tallentanut. Kiistämättömyydellä pyritään varmistamaan tietojen luotettavuus ja alkuperä tallentamalla tietoa siitä, kuka tiedon on luonut. Pääsynvalvonta (eng. access control) tarkoittaa tietojärjestelmän kykyä tunnistaa tietojärjestelmiä käyttävä henkilö. Pääsynvalvonta on keskeinen asia verkottuneessa tietojenkäsittely-ympäristössä. (Hakala ym. 2006, 5.) Kuviossa 1 on kuvattu tiedon turvallisuuteen liittyvät ulottuvuudet.

Kuvio 1: Tiedon turvallisuuden ulottuvuudet



Pelkän tiedon käsitteestä on nykymaailman tarpeiden vuoksi tietoturvallisuuden määritelmää laajennettu käsittämään tietojen käsittelyä varten käytetyt laitteet ja näiden tietoliikennejärjestelmät. Näissä käsitteissä on huomioitu tietoliikennejärjestelmien suojaaminen myös sellaisilta luvattomilta käyttäjiltä, jotka eivät sinänsä ole kiinnostuneita organisaation varsinaisesta tiedollisesta pääomasta mutta haluavat käyttää luvatta hyväkseen olemassa olevia tiedonkäsittelyinfrastruktuureja. (Hakala ym. 2006, 4.) Tietojärjestelmiä koskevasta tietoturvallisuuden ulottuvuudesta käytetään myös käsitettä ”tietotekniikan turvallisuus”. (Valtionvarainministeriö, 2008.) Synonyymina voidaan käyttää myös käsitettä ”tietojärjestelmäturvallisuus”.

Tietojärjestelmiin tallennetun tiedon lisäksi järjestelmiin tallennetaan tietoja tietojen käsittelijöistä ja erilaisia lokeja. Tällaista tietoa kutsutaan metatiedoksi. Metatieto on ”tietoa tiedosta”, eli varsinaisen käyttötiedon, kuten dokumentin sisällön, ympärillä olevaa sivutietoa, joka pitää sisällään esimerkiksi tietoja siitä, kuka tietosisältöä on käsitellyt, luonut tai poistanut. Metadataa tallentuu erityisesti toimistoympäristössä käytettäviin dokumenttitiedostoihin ja ne pitävät sisällään tietoa mm. siitä, kuka tiedoston on luonut, missä organisaatiossa, miten tiedostoa on muokattu, mitä mallipohjaa tiedostoon on käytetty, milloin tiedosto on laadittu ja joissakin tapauksissa myös poistettuja tekstinkappaleita. (Volonino & Anzaldua 2008, 202.)

3.2 Tietoturvallisuus pienessä yrityksessä

Suomalaisista yrityksistä 99 % on Tilastokeskuksen määritelmän mukaisia pieniä yrityksiä henkilöstömääränsä osalta. Yrityksiä, jotka koostuivat 0-9 henkilöstä oli Suomessa vuonna 2012 yhteensä 303 931 kappaletta, ja 10-49 työntekijän yrityksiä 15 083 kappaletta. Yhteensä yrityksiä oli Suomessa kyseisenä vuonna 322 183 kappaletta, joten pienet yritykset ovat selkeästi suurin yksittäinen yrityskoko. Näistä yrityksistä alle kymmenen hengen yritykset ovat edelleen tilastollisessa valta-asemassa. (Tilastokeskus 2013.)

Yrityksillä, joiden palveluksessa on nolla henkilöä, tarkoitetaan Tilastokeskuksen määritelmässä ilmeisesti niin sanottuja ”pöytälaatikkoyrityksiä”. Pöytälaatikkoyritys on yritys, jolla ei ole työntekijöitä tai olemassa olevaa liiketoimintaa (Taloussanomat 2014).

Pienyrityksen tietoturvallisuussuunnittelu tehdään samoista yleisistä peruslähtökohdista kuin suuressakin organisaatiossa. Tietoturvallinen toiminta on osa yrityksen elinkelpoisuutta ja tärkeän tiedon turvaaminen on yritykselle menestymisen edellytys. Myös pienissä yrityksissä on paljon suojattavaa tietoa (Viestintävirasto 2013.)

Voidaan olettaa, että erityisesti pienyrityksessä toteutunut sisäinen tai ulkoinen tietoturvauhka voi lopettaa liiketoiminnan kerralla, sillä kyky toipua yritystoimintaan kohdistuvista häiriöistä on todennäköisesti pienemmästä taloudellisesta mukautumiskyvystä johtuen suurempia yrityksiä heikompi.

Tietoturvallisuutta uhkaava kyberrikollisuus on maailmanlaajuisesti jo huumausainekauppaa suurempi tulonlähde rikollisille. Interpolin mukaan pelkästään Euroopassa kyberrikollisuudessa liikkuu rahaa noin 750 miljardia euroa. Esimerkkeinä näistä kyberrikollisuuden alalajeista ovat laiton uhkapeli, luottokorttipetokset sekä pankkeihin ja yrityksiin kohdistuvat tietoverkkorikokset. Pankkiryöstötkin ovat siirtyneet verkkoon – perinteisillä ”pyssy ja mies”-menetelmillä yhdysvaltalaisista pankeista varastettiin vuonna 2012 900 miljoonaa dollaria, mutta kyberrikoksilla tehdyt varkaudet ylittivät jo 12 miljardin dollarin summan. Britanniassa yli 90 % suurista yrityksistä on joutunut vuonna 2012 kyberrikollisten hyökkäyksen kohteeksi. Sekä FBI että Interpol kertovat, että kyberrikollisuus on nopeimmin kasvavia rikollisuuden muotoja. (Helsingin Sanomat 2014.)

Tietoturvallisuuden hallinta ei ole pelkästään, eikä edes enimmäkseen, teknisiä ratkaisuja, vaan kyse on pääsääntöisesti siitä, miten yrityksessä ylipäänsä työskennellään tiedon kanssa ja miten yrityksen työntekijät käsittelevät yrityksen hallussa olevia tietoja. Tietoturvallisuudesta huolehtiminen on kaikkien yrityksen työntekijöiden vastuulla. Tärkeää tietoa on sähköisten järjestelmien lisäksi myös paperilla ja puhuttuna. Tietoturvallisuuden hallitseminen edellyttää myös tällaisten, ei-sähköisten tietojen turvallista käsittelyä. Hyvä tietoturva ei vaadi suuria panostuksia, vaan pienelläkin panostuksella voidaan hyödyttää liiketoimintaa. (Viestintävirasto 2014.)

3.2.1 Tietoturvapolitiikka ja -suunnitelma

Organisaatiossa tavoiteltava tietoturvataso ja sitä koskevat näkemykset esitetään yrityksen tietoturvapolitiikassa, joka on asiakirja joka sisältää tietoturvallisuutta koskevat ohjeet ja periaatteet koko organisaation tasolla. Tietoturvapolitiikka toimii tietoturvallisuusohjeita ohjaavana, yläkäsitemäisenä dokumenttina, jonka perusteella laaditaan tietoturvaohjeet ja

-käytännöt. Tietoturvapolitiikan laatimisesta vastaa yrityksen johto tai tietohallinto-osasto, mikäli yrityksessä on sellainen. (Andreasson & Koivisto 2013, 34.)

Yrityksen johdon tietoturvallisuusjohtamisen perustana on ajantasainen tietoturvapolitiikka. Tietoturvatoimintaan kuuluu säännöllinen riskien arviointi- ja hallintatyö, uusien järjestelmien tietoturvatason määrittely ja näihin järjestelmiin liittyvien tietoturvariskien hallinta koko laitteiston elinkaaren ajan. (Valtionvarainministeriö 2007, 28.)

Tietoturvapolitiikassa tulee teknisten määritelmien sijaan korostaa erityisesti tiedon turvallista käsittelyä työntekijöiden ja organisaation toimesta. Kirjallisen tietoturvapolitiikkadokumentin osa-alueiksi kirjataan ainakin johdanto, tietoturvapolitiikan tavoite, tietoturvatoimintaa ohjaavat tekijät, tietoriskien hallinta ja tietoturvallisuuden merkitys organisaatiolle. Näiden lisäksi politiikkaan kuuluvat turvatoimien priorisointi, tietoturvallisuuden hallintajärjestelmät, tietoturvavastuut, tietoturvakoulutus- ja ohjeet. Myös tietoturvallisuudesta tiedottaminen, tietoturvallisuuden toteutumisen valvonta sekä toiminta poikkeustilanteissa ja –oloissa ovat osa tietoturvapolitiikkaa. Tietoturvapolitiikka on strategisen tason dokumentti, jossa kuvataan tavoiteltavat tasot hyväksyttävän tietoturvallisuuden saavuttamiseksi ja ylläpitämiseksi. (Andreasson & Koivisto 2013, 35-36.)

Tietoturvapolitiikan perusteella laaditaan yrityksen tietoturvasuunnitelma, joka sisältää ne käytännön ratkaisut joilla tietoturvapolitiikan määrittelemiin tavoitteisiin päästään. Tietoturvasuunnitelmassa kuvataan yksityiskohtaisesti ne menetelmät ja tekniset ratkaisut joita yrityksessä käytettävissä järjestelmissä toteutetaan. (Hakala ym. 2006, 9.)

Tietoturvasuunnitelman apuna voi käyttää tietoturvallisuuteen liittyviä malleja tai standardeja. Standardit eivät tarjoa valmista mallia tietoturvasuunnitteluun, mutta ne auttavat tietoturvallisuuden suunnittelun menettelytapojen rakentamisessa. Standardien perusteella voidaan määritellä mitä suunnittelutyöhön sisältyy ja missä muodossa siitä saatavat tulokset esitetään. (Hakala ym. 2006, 46.)

3.2.2 Tietoturvaohjelma

Pienissä yrityksissä, joissa työntekijöitä on vähän tai joissa ei välttämättä ole yrityksen omistajan lisäksi muita työntekijöitä, tietoturvapolitiikka ja tietoturvasuunnitelma voidaan tiivistää yhteen dokumenttiin tietoturvaohjelmaksi. Tietoturvaohjelma on dokumentti, johon keskeiset tietoturvallisuutta koskevat asiat voidaan kerätä. Erillisen politiikan ja suunnitelman sijaan yksittäinen tietoturvaohjelma on kevyempi hallita ja sisältää pienissä yrityksissä usein kaiken tarpeellisen hyvän tietoturvallisuustason ylläpitämiseksi. (Viestintävirasto 2013.)

Tietoturvaohjelman keskeisiä avainkohtia ovat yrityksen johdon kannanotto tietoturvallisuuteen, suunnitelman tarkoituksen ja tärkeyden kuvailu, suunnitelman piirissä olevien tahojen tarkka erittely, salassapito- ja kilpailukieltosopimukset avainhenkilöiden ja yhteistyökumppanien kanssa ja suojattavan aineiston määrittely. Tietoturvaohjelmaan on hyvä kirjata myös tiedon luokitteluperiaatteiden määrittely, tietoturvasta vastaavan henkilö sekä toimintaohjeet toteutuneiden tietoturvauhkien varalta. Myös tiedon käsittelyyn, säilyttämiseen, välittämiseen, kirjaamiseen, kopiontiin ja hävittämiseen liittyvät periaatteet ja menettelytavat sekä tietoturvallisuuteen liittyvän koulutuksen järjestäminen määritellään tietoturvaohjelmassa. (Viestintävirasto 2013.)

3.2.3 Tietosuoja ja henkilötietojen käsittely

Mikäli yritys käsittelee toiminnassaan henkilötietoja sellaisella tavalla, että kootuista henkilötiedoista muodostuu henkilörekisteri, tulee yrityksen ottaa huomioon tietosuojan ja henkilötietolain luomat velvoitteet. Henkilörekisterin käsittelyyn liittyy useita lain mukanaan tuomia velvollisuuksia, joista henkilörekisterin käsittelijän on oltava tietoinen. Tavanomainen yritys muodostaa usein henkilörekisterin esimerkiksi asiakas- tai henkilöstötietojensa pohjalta. Näiden tietojen kerääminen riittää täyttämään henkilörekisterin kriteerit, jolloin yrityksestä tulee rekisterinpitäjä. (Tietosuojavaltuutettu 2014.)

Rekisterinpitäjän velvollisuudet ja oikeudet muodostuvat henkilötietolain perusteella. Laki koskee sekä viranomaisten että yritysten kuin järjestöjen, yhteisöiden ja yksityistenkin henkilöiden toimintaa. Laissa on kuitenkin rajattu lain soveltamisalan ulkopuolelle yksityishenkilöiden vähäinen henkilötietojen keruu, joten esimerkiksi ystävien yhteystiedoista koostuva lista ei ole lain tarkoittama henkilörekisteri. Yritystoiminnassa asiakasrekisteri tai yhteystietorekisteri kuitenkin on sellainen. Henkilötietolaki kertoo, milloin yritys voi kerätä tai käsitellä henkilötietoja. Lain asettamat velvoitteet, kuten suunnittelu-, tarpeellisuus-, huolellisuus- ja suojaamisvelvoitteet määrittelevät ne puitteet joissa henkilötietoja voidaan käsitellä. Näitä puitteita seuraamalla on mahdollista saavuttaa jo hyvä tietojenkäsittelytapa, joka turvaa käsiteltäviä henkilötietoja. (Tietosuojavaltuutettu 2014.)

Henkilötietojen suojaamisen velvoite on osa henkilötietojen käsittelyprosessia. Velvoitteen sisältö tulee arvioida henkilötietojen keräämisen tarkoituksen kautta. Henkilötietoja saa kerätä ja käsitellä ainoastaan siinä laajuudessa ja sitä tarkoitusta varten mitä varten yritykset niitä tosiasiallisesti tarvitsevat. Ylimääräisten tietojen kerääminen ja käsittely on kielletty. Henkilötietolakia sovelletaan myös tietoverkossa tapahtuvaan henkilötietojen käsittelyyn. Siten esimerkiksi verkkokaupat, postituslistat ja keskustelupalstat kuuluvat henkilötietolain soveltamisalan piiriin. Yrityksen on syytä varmistaa, että heillä on oikeus kerätä, käyttää tai käsitellä niitä henkilötietoja joita yritykselle toiminnassaan kertyy. Henkilötietojen kerääminen edellyttää keräämisen kohteelta yksilöityä, vapaaehtoista ja tietoista suostumusta. Jos

suostumusta ei erikseen kysytä, rekisteriä voi myös kerätä silloin, kun yrityksen ja keräämisen kohteen välillä on asiallinen yhteys esim. asiakkuuden, jäsenyyden tai muun vastaavan sellaisen suhteen perusteella johon keräämisen kohden on itse suostunut. Henkilötietoja ei saa kerätä salaa eikä ilman lupaa. (Tietosuojavaltuutettu 2014.)

Arkaluontoisten tietojen kerääminen on pääsääntöisesti kielletty. Arkaluontoisiin tietoihin kuuluvat henkilön rotua tai etnistä alkuperää, uskonnollista tai poliittista vakaumusta, ammattiliittoon kuulumista, rikollista tekoa tai rangaistusta, terveydentilaa, seksuaalista suuntautumista tai sosiaalihuollon palveluita koskevat tiedot. Mikäli tällaisten tietojen käsittelyyn on kuitenkin asiallinen tarve, on näitä tietoja käsittelevät yrityksen selvitettävä huolellisesti syntyykö tietoihin käsittelyoikeus. (Tietosuojavaltuutettu 2014.)

Rekisteröidyillä henkilöillä itsellään on lain suomia oikeuksia suhteessa heistä kerättyihin tietoihin. Rekisteröity saa tarkastaa itseään koskevat tiedot ja vaatia virheellisen tiedon oikaisua. Lisäksi rekisteröity saa kieltää henkilötietojensa käsittelyn suoramarkkinointiin, markkina- ja mielipidetutkimuksiin, henkilömatrikkeliin ja sukututkimukseen. Tästä kieltooikeudesta pitää antaa tieto rekisteröimisen yhteydessä. Tämän lisäksi markkinointi sähköpostin tai matkapuhelimen välityksellä on sallittu ainoastaan erillisellä, etukäteen saadulla suostumuksella. (Tietosuojavaltuutettu 2014.)

Rekisterinpitäjän on laadittava jokaisesta henkilötietolain tarkoittamasta rekisteristä rekisteriseloste, jonka pitää olla kaikkien saatavilla. Sen voi liittää esimerkiksi yrityksen verkkosivuille. Rekisteriselosteen laatiminen luo luottamusta yritykseen ja osoittaa, että yritys toimii avoimesti ja tuntee velvollisuutensa. Henkilötietojen käsittelyä valvoo tietosuojavaltuutettu. Henkilötietojen käsittelyä varten käytetyt tietojärjestelmät pitää suojata asianmukaisesti henkilötietojen leviämisen estämiseksi. (Tietosuojavaltuutettu 2014.)

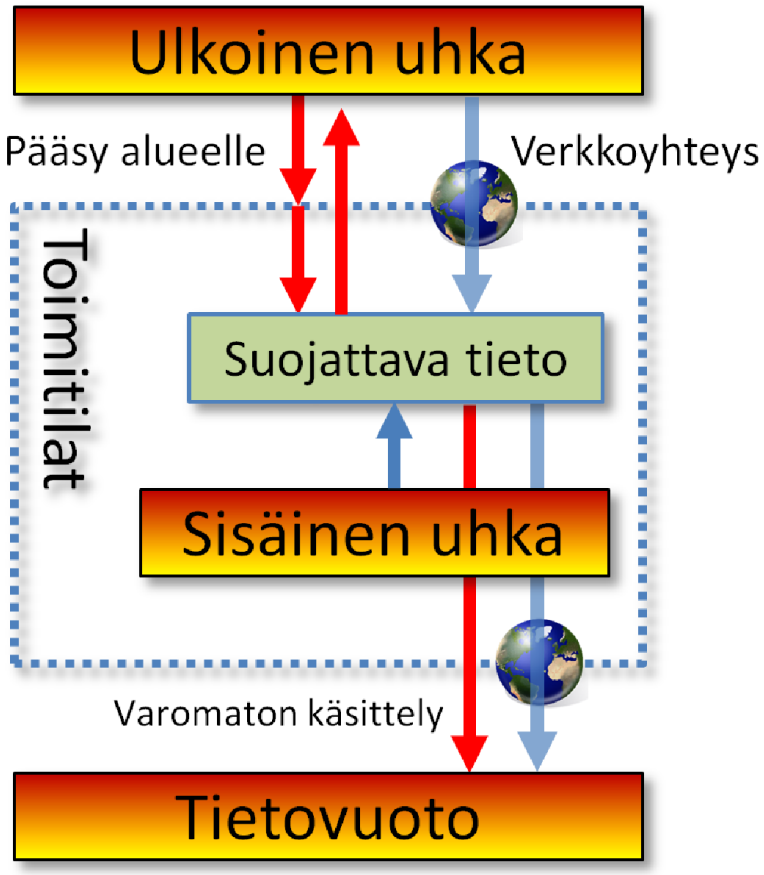
Tietojärjestelmien tietoturvallisuutta suunnitellessa on otettava huomioon myös tietojenkäsittelyyn liittyvä, yrityksiä velvoittava juridinen puoli. Järjestelmien halutaan kertovan luotettavasti sen, kuka järjestelmässä olevan tiedon on luonut. Tämä on tärkeää esimerkiksi kaupankäynnin tai muun sähköisen asioinnin luotettavuudessa. (Hakala ym. 2006, 4.)

3.3 Ulkoinen ja sisäinen tietoturvauhka

Ulkoinen tietoturvauhka tarkoittaa tietoturvaloukkausta. Yleisimpiä rikosnimikkeitä tietoturvaloukkaustapauksissa ovat luvaton käyttö tai vaaran aiheuttaminen tietojenkäsittelylle (Lagus 2013). Myös tietomurto, tietoliikenteen häirintä sekä viestintäsalaisuuden loukkaus ovat rikosnimikkeitä, joiden tunnusmerkistö toteutuu tietoturvaloukkauksina pidettävissä tietoverkkorikoksissa (Sanastokeskus 2004, 19). Tietoturvallisuutta koskevia rikoksia koskevat pykälät on pääsääntöisesti kirjattu Rikoslain 38 lukuun tieto- ja viestintärikoksista.

Ulkopuolelta tuleviin tietoturvauhkiin käytetyt, keskeiset väylät ovat luvaton fyysinen pääsy alueelle sekä luvaton pääsy tietojärjestelmiin internetin kautta. Kuviossa 2 on esitetty sisäisen ja ulkoisen tietoturvauhan keskeiset väylät suojattavan tiedon luokse.

Kuvio 2: Sisäisen ja ulkoisen uhan väylät



Luvaton pääsy tietojärjestelmiin voi tapahtua myös yrityksen sisältä, jolloin kyseessä voi olla sisäinen tietoturvauhka. Rikollisen intressin lisäksi suojattavat tiedot voivat lähteä organisaation käsistä myös joko inhimillisen virheen tai ohjelmiston toimintavirheen vuoksi vahingossa, jolloin puhutaan tietovuodosta (Uusi Suomi 2014).

Yrityksen henkilökunnalla saattaa olla rikollinen intressi tietoon, joka yrityksessä on suojattu. Siksi hyvään tietoturvahallintaan kuuluu myös fyysinen ja tietojärjestelmäratkaisuin toteutettu pääsynrajoittaminen yrityksen sisällä. Keinoja pääsynrajoittamiseen ovat pääsyn rajaaminen palvelintiloihin tai alueelle joissa käsitellään suojattavaa tietoa, kuvallisten henkilökorttien käyttö yrityksen tiloissa, kulunvalvonnan rajaaminen alueilla joissa käsitellään suojattavaa tietoa sekä ennen kaikkea suojattavan tiedon käsittelyyn varattujen tilojen, kuten palvelinhuoneiden, riittävä fyysinen suojaaminen. Mikäli yrityksessä on työntekijöitä, joilla ei työtehtäviensä puolesta ole tarvetta päästä palvelinhuoneisiin, heiltä on syytä rajata kulkuoi-

keudet pois näistä huoneista. Uusien työntekijöiden kohdalla on harkittava turvallisuusselvityksen teettämistä, mikäli työntekijät käsittelevät työssään suojattavaa aineistoa. (Tipton & Krause 2007, 742-744.)

Tietoverkoissa pääsyn rajaaminen voidaan tehdä käyttämällä tarkoitukseen sopivia keinoja kuten Microsoft Windows-ympäristössä käytettävää Active Directory- käyttäjänhallintajärjestelmää. Järjestelmän avulla voidaan rajata työntekijöiden pääsyä jaettuihin verkkoresursseihin tai tietokantoihin siten, että suojattavaa dataa käsittelevät vain ne käyttäjäryhmät, joilla on siihen työtehtäviensä perusteella tarve. Tietoverkkojärjestelmät ja niihin liitetyt laitteet voidaan turvata rajaamalla käytettäviä ohjelmistoja vain erikseen hyväksyttyihin ja sulkemalla pois ylimääräinen verkkoliikenne. Käytettävien ohjelmistojen ja laitteiden tietoturvahaavoittuvuuksia pitää seurata aktiivisesti, järjestelmien lokitietoja pitää tarkkailla ja käytöstä poistettujen tietovälineiden tietoturvallinen hävittäminen on varmistettava käyttämällä datan hävittämiseen tarkoitettuja ohjelmistoja ja laitteita. Vähintään sisäverkon ja ulkoverkon reuna-alueelle on sijoitettava palomuuri, joka rajaa ulkopuolelta tulevaa verkkoliikennettä. Sisäverkon jakaminen toisistaan palomuurilla suodatettuihin eri suojausalueisiin on myös mahdollista. (Tipton & Krause 2007, 745-749.)

Sisäisellä tietoturvauhalla tarkoitetaan organisaation sisäisistä tapahtumista johtuvia riskejä, jotka uhkaavat tietoturvallisuutta. Sisäisissä tietoturvauhissa ei yleensä ole aktiivista toimijaa, joka pyrkii vahingoittamaan yritystä tai kaappaamaan sen tietoja. Tyypillinen esimerkki sisäisestä tietoturvauhasta on puutteellisesti toteutettu varmuuskopiointi, joka altistaa yrityksen tietojen menetykselle laiterikon tapahtuessa. Tietokoneet ja tietojärjestelmät tallentavat tiedon tallennusmedioille niin, että ne säilyvät siellä myös virransyötön katkettua, mutta tiedontallennusvälineet ovat mekaanisina laitteina vikaantumisalttiita. Mikäli yrityksen kaikki tiedollinen pääoma on yhdellä jaetulla verkkolevyllä, jota ei ole varmuuskopioitu, voidaan kaikki nämä tiedot menettää kyseisen levyn vikaannuttua. Levy voi myös ajan mittaan kulua siten, että sen levypinta-alasta yhä suurempi osa muuttuu luku- ja kirjoituskelvottomaksi. Usein tiedostot ovat pelastettavissa apuvälineillä tai asiaan perehtyneiden asiantuntijoiden toimesta, mutta tiedon saatavuus ainakin tässä välissä on heikentynyt. Myös inhimillisen vahingon mahdollisuus tiedon hävittämisessä on otettava huomioon. (Korpela 2005, 96.)

Yksi tapa varmistaa yhdellä levyllä säilytettävät tiedot on tehdä niistä manuaalisesti määräajoin kopio toiselle levylle, jolloin päälevyn vikaantuessa tiedot voidaan palauttaa varalevyltä. Tiedontallennusratkaisuissa on myös saatavissa levyjärjestelmiä, joissa tiedon kahdennus tapahtuu automaattisesti käyttäjän asiaan puuttumatta. Tämä paikallinen turvallisuusratkaisu suojaa yhden kovalevyn rikkoutumiselta, ja sitä voidaankin pitää tärkeän tiedon suojaamisen minimitasona. Myös tulipalo voi vahingoittaa tallennusvälineitä, jolloin paikallisesti varmistettu tiedontallennusalusta voi tuhoutua kokonaisuudessaan jolloin myös varalevy vaurioituu käyttökelvottomaksi. (Korpela 2005, 96.)

Organisaatiossa, jossa tietoa käsitellään paljon tai jossa käsittelijöitä on monta, on syytä luoda automaattinen varmistusjärjestelmä esimerkiksi siten, että tiedot tallentuvat automaattisesti tietoverkon yli keskitettyyn, varmistettuun tiedontallennuspalvelimeen. Tällainen järjestely on käyttäjälle näkymätön, eikä aiheuta järjestelmän käyttäjälle ylimääräistä vaivaa. (Laaksonen 2006, 170.)

Internetissä on tarjolla erilaisia pilvipalveluita, joihin tietoa voidaan tallentaa siten, että kopio tiedoista päivittyy automaattisesti toisaalla olevalle palvelimelle. Tällöin myös katastrofaalisen tuhoutumisen aiheuttamat tietoturvallisuusriskit saadaan hallittua, ja arvokas tieto on taltioitu. (Korpela 2005, 96.)

Tiedon tallentamisessa pilvipalveluun on kuitenkin omat riskinsä, sillä silloin yrityksen tietojen hallinta luovutetaan kolmannelle osapuolelle. Erityisesti arkaluontoisen ja huolellisesti suojattavan tiedon taltioiminen pilveen sisältää paljon riskejä, joten hyödyn ja haitan punninta on tehtävä tarkasti. Paikallisissa varmuuskopiointiratkaisuissa tätä riskiä ei ole. Pilvipalveluun tallennettu tieto voi myös kadota palveluntarjoajan laitejärjestelmän vikatilanteissa tai pilvipalvelun käyttöä varten tarvittavat käyttäjätunnukset voidaan saada luvattomasti haltuun jolloin tiedot paljastuvat ulkopuolisille. Pilvipalveluihin taltioitu tieto on aina varmistettava vähintään paikallisesti, eikä pilvipalvelua voikaan tietoturvallisesti käyttää tiedon ainoana tallennuspaikkana. (Kirchgaessner 2013.)

4 Tietoturvallisuuden hallinnan osa-alueet

Tietoturvallisuuden kokonaisuuden hallinta ei rajoitu ainoastaan yrityksen tietojärjestelmien tekniseen suojaamiseen. Tietoturvallisuus on osa yrityksen kokonaisturvallisuutta, ja tätä voidaankin havainnollistaa pilkkomalla tietoturvallisuus helpommin hahmotettaviksi osa-alueiksi. Näitä osa-alueita ovat yleisesti käytettyjen määritelmien mukaan hallinnollinen turvallisuus, fyysinen turvallisuus, henkilöturvallisuus, laitteisto- ja tietoliikenneturvallisuus, ohjelmistoturvallisuus ja tietoaineistoturvallisuus. (Hakala ym. 2006, 10-12.)

Valtionhallinnon kansallisessa turvallisuusauditointikriteeristössä (KATAKRI) yrityksen turvallisuustoiminnot on jaettu siten, että tietoturvallisuus käsittää yllä olevista kategorioista laitteisto- ja tietoliikenneturvallisuuden, ohjelmistoturvallisuuden ja tietoaineistoturvallisuuden alle kuuluvat asiat. Hallinnollinen, fyysinen ja henkilöstöturvallisuus käsitetään osaksi yrityksen yleistä turvallisuuskriteeristöä. (Puolustusministeriö 2011.)

4.1 Hallinnollinen turvallisuus

Hallinnollinen turvallisuustyö on turvallisuusjohtamista. Hallinnollisessa turvallisuustyössä tulee huomioida kaikkien turvallisuuden osa-alueiden vaatimukset, eli turvallisuuden osa-alueita

ei voi käsitellä yksittäisinä, itsenäisinä kokonaisuuksina (Puolustusministeriö 2011, 3). Nykyaikaisella yritysjohtajalla tulee olla tietotaitoa taloushallinnon ja henkilöstöhallinnon lisäksi myös tietotekniikan ja tietoturvallisuuden alueilta. Hyvä, malleihin ja standardeihinkin perustuva tietoturvallisuusjohtaminen on tehotonta, mikäli tietoturvallisuutta johdetaan liiketoiminnan muusta johtamisesta irrallisena osa-alueena. Tietoturvallisuus kuuluu päivittäisjohtamiseen, ja se on otettava huomioon osana jokaisen yrityksen työntekijän päivittäisiä työtehtäviä. (Laaksonen ym. 2006, 116.)

Tietoturvallinen toiminta voidaan liittää osaksi työntekijöiden päivittäisiä tehtäviä, eikä sitä tarvitse silloin kouluttaa erillisenä asiana. Mikäli tietoturvalliset toimintatavat koulutetaan normaaleiksi tavoiksi käsitellä tietoa, säästetään aikaa ja resursseja erillisiltä, tietoturvaan liittyviltä lisäkoulutuksilta. Yrityksen johdon on tarkoin harkittava, millaisilla toimintatavoilla saavutetaan tasapaino tietoturvallisen toiminnan ja yrityksen perustoiminnan välillä. Tietoturvallinen toiminta ei saa muodostua liialliseksi rasitteeksi perustoiminnalle, jotta sitä voidaan noudattaa eikä yrityksen tuottavuus heikkene. Toimiva tietoturvallisuus liitetään toimivaksi osaksi yrityksen perusprosesseja ja tämän liitoksen tekeminen on yrityksen hallinnon tehtävä. (Laaksonen ym. 2006, 116.)

Hallinnollisen turvallisuuden tehokkaalla toteuttamisella pyritään varmistamaan se, että tietoturvallisuus on yrityksessä aktiivisesti johdettua toimintaa. Tämän lisäksi hallinnolliseen turvallisuuteen kuuluu tietoturvan jatkuva kehittäminen ja ylläpito. Tietoturvallisuus on prosessi, jonka omistajana on yrityksen johto tai johdon tätä tarkoitusta varten osoittama taho. (Hakala ym. 2006, 11.)

Yrityksen tietoturvapolitiikan ja -suunnitelman laatiminen on tärkein osa hallinnollista turvallisuutta ja sitä voidaan pitää hallinnollisen turvallisuustyön perustasona. Suunnitelmista on selvittävä, mitä turvallisuuden osatekijöitä turvallisuuspolitiikka ja turvallisuuden johtaminen yrityksessä kattaa. Turvallisuusdokumentaation on vastattava sitä toimintaa, mitä yrityksessä tosiasiassa tapahtuu. (Puolustusministeriö 2011, 8.)

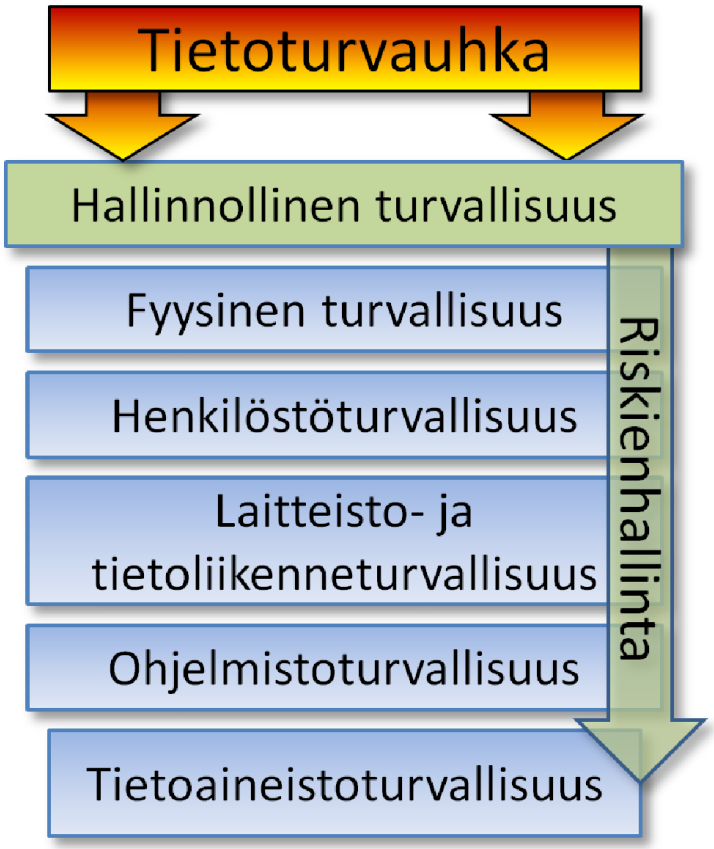
Hallinnollisella tasolla on otettava myös huomioon, että tietoturvallisuusnäkökulmat huomioidaan lainsäädännön sekä yksityisoikeudellisten sopimusten näkökulmasta. Pienissä yrityksissä tämä tehtävä kuuluu yrityksen toimitusjohtajalle, suuremmissa yrityksissä tehtävä kuuluu yrityksen tietohallinto-osastolle. Hyvin toteutettu hallinnollinen turvallisuus on toimivan tietoturvallisuuskulttuurin kivijalka. (Hakala ym. 2006, 11.)

Organisaatioiden riskikartoituksissa tietoturvallisuuteen liittyvät riskit nousevat keskeisiksi osa-alueiksi. Yritysten tietoturvariskien hallintaa vaikeuttaa se, että riskit ovat usein riippuvaisia kolmannen osapuolen palveluntuotannosta, sillä monet erilaiset palvelu- ja sopimustoimittajat toimittavat yrityksen käyttöön laitteistoja ja ohjelmistoja, joissa olevia riskejä

yritys ei pysty itse täysin hallitsemaan. Yritys on riippuvainen siitä, että esimerkiksi ohjelmiston tuottaja pitää huolen ohjelmiston tietoturvasta ja toimittaa yrityksen saataville ajantasaisia versioita joissa uudet tietoturvahaavoittuvuudet on paikattu. Hallinnollisella tasolla on otettava huomioon, että myös kolmansien osapuolien toimittamat ratkaisut kuuluvat yrityksen kokonaisvaltaiseen tietoturvariskien hallintaan, ja käytettävien ohjelmistojen versionhallinta on osa tietoturvallisuussuunnittelua. Näiden palveluiden mukanaan tuomat riskit pitää hallita jo sopimusvaiheessa ja siten varmistaa, että poikkeustilanteet on huomioitu jo sopimuksia laadittaessa. (Andreasson & Koivisto 2013, 38.)

Tietoturvallisuuden hallintaa voidaan ajatella kerrosmallina, jossa ylempien kerrosten asiallinen hoitaminen tukee alempien kerrosten ratkaisuja alla olevan kuvion 3 mukaisesti.

Kuvio 3: Tietoturvallisuuden hallinnan osa-alueiden kerrosmalli



Voidaan ajatella, että tietoturvallisuuden kokonaisvaltainen hallinta edellyttää ylemmillä tasoilla tehtävää perusturvallisuustyötä jotta niiden alaisuuteen kuuluvat osa-alueet voidaan turvata. Keskeinen asia alempien kerrosten tehokkaassa hoitamisessa on toimiva turvallisuusjohtaminen eli hallinnollinen turvallisuus, josta riskienhallintatyö ulottuu alempien kerrosten läpi kohti tietoaineiston suojaamisen tavoitetta.

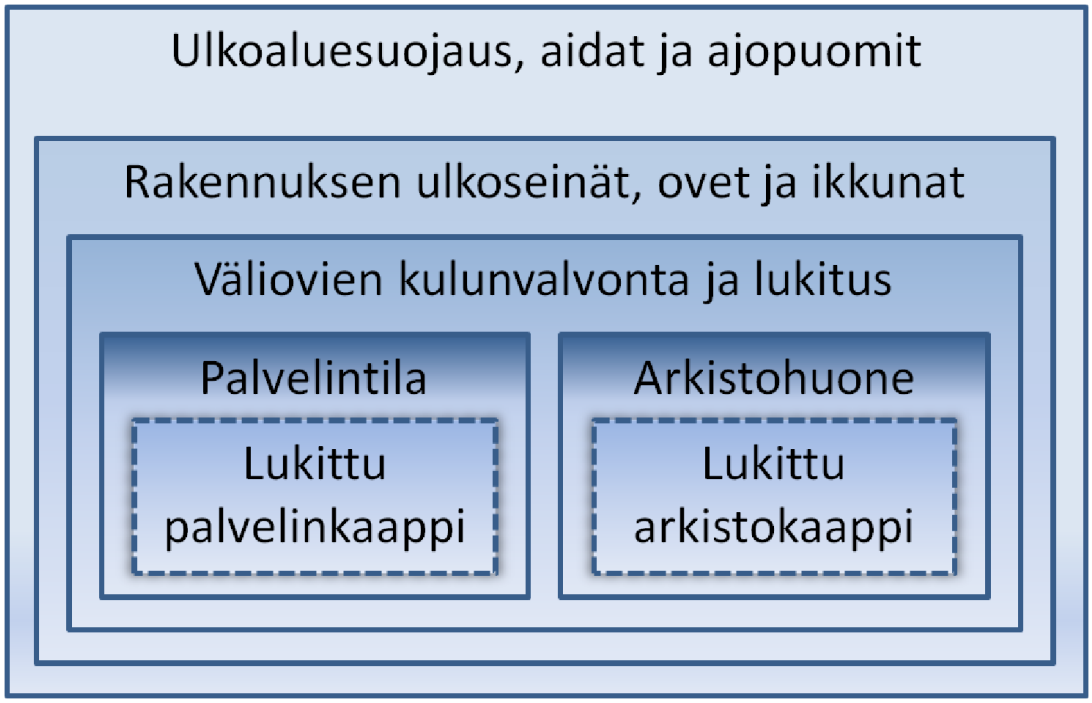
4.2 Fyysinen turvallisuus

Fyysisellä turvallisuudella tarkoitetaan ensisijaisesti toimitilojen turvallisuuteen liittyviä seikkoja. Fyysisen turvallisuuden tietoturvallisuusulottuvuutena on suojata suojattavia tietoja estämällä pääsy tietoihin mahdollisimman varhaisessa vaiheessa. Fyysisen turvallisuuden vaatimuksia tiukennetaan sitä enemmän, mitä lähemmäs suojattavaa ainestoa päästään. Tärkeimpiä suojattavia kohteita ovat tietojärjestelmien kriittisiä osia sisältävät laitetilat. (Puolustusministeriö 2011, 60.)

Fyysinen turvallisuus sisältää rakennukseen sijoitettujen laitteiden turvallisuudesta huolehtimisen. Se sisältää tietoturvaloukkauksilta suojautumisen lisäksi ympäristön häiriöiltä suojautumisen elementin. Fyysisen turvallisuuden suunnittelussa on otettava huomioon murtovarmuus, vesi- ja palovahinkojen vaikutuksilta suojautuminen sekä sähkö- ja lämmitysjärjestelmien häiriöitten ja vikatilojen sietäminen. Fyysisen turvallisuuden ylläpidosta vastaa pääsääntöisesti kiinteistön isännöinti- ja vartioimispalveluita tuottava taho, mutta yrityksen käytössä olevien laitteistojen asianmukainen suojaaminen jää yrityksen itsensä suunniteltavaksi. Jos yrityksen tiloissa on esimerkiksi palvelinsali, tulee tällainen sali suojata asiantuntevan, tietojärjestelmien turvallisuussuunnittelun ammattilaisen avulla. (Hakala ym. 2006, 11.)

Kuviossa 4 on havainnoillistettu esimerkki tiedon fyysisistä suojauskerroksista. Tunkeutujan on läpäistävä kaikki suojauskerrokset suojattavan tiedon saavuttamiseksi.

Kuvio 4: Suojattavan tiedon suojauskerrokset



Tietojärjestelmien häiriöttömän sähkönsyötön turvaaminen on osa fyysistä tietoturvallisuutta. Sen tavoitteena on varmistaa, etteivät ympäristöstä tai säätilasta johtuvat virtapiikit hajota laitteistoja tai ettei esimerkiksi sähkökatkos sulje laitteistoja hallitsemattomasti. Joillakin yrityksillä yrityksen pääasiallinen tuote on verkkopalvelu, jolloin sähkökatkos tekee palvelusta käyttökelvottoman. Tämä voidaan estää käyttämällä varmistettua sähkönsyöttöä, jolloin sähkökatkon tai muun virtahäiriön sattuessa riittävä virransaanti on varmistettu esimerkiksi varavirtakoneiden tai UPS-laitteiden (eng. Uninterruptable Power Source) avulla. (Hakala ym. 2006, 309-314.)

Osa fyysistä turvallisuutta on toimitilojen käyttöturvallisuus, jonka piiriin kuuluu sen varmistaminen, ettei toimitiloissa työskenteleviin henkilöihin kohdistu puutteellisesta tilaturvallisuussuunnittelusta johtuvia riskejä. Se sisältää kaikki ne rakenteelliset ja valvonnalliset ratkaisut, joilla varmistetaan tietoteknisten laitteiden ja järjestelmien pysyminen vain niihin oikeutettujen henkilöiden hallinnassa ja käytössä. Rakenteelliset ratkaisut tarkoittavat kiinteistön seiniä, ovia, ikkunoita, lukkoja ja muita mekaanisia esteitä. Valvonnalliset ratkaisut käsittävät kulunvalvonnan, vieraiden saattamisen, videovalvonnan ja murtohälyttimien kaltaiset ratkaisut. Kulunvalvonnalla voidaan kerätä tietoa siitä, kuka tiloissa liikkuu ja milloin. Lisäksi sillä voidaan ohjata lukkoja siten, että asiattomien pääsy toimitiloihin estyy. Kulunvalvontaan yhdistetty murto- ja videovalvonta tukee kokonaisuutena toimitilojen turvallista käyttöä kytkemällä murtohälytinjärjestelmän automaattisesti päälle ja keräämällä videovalvonta-aineistoa tilojen käyttäjistä. Lukittu ulko-ovi ja toimivat murtohälyttimet ovat osa tietoturvallisuuden kokonaisuuden ylläpitoa, sillä varastettu, suojaamaton tietokone on sekä omaisuushävikkiä että tietoturvariski. (Andreasson & Koivisto 2013, 53-64.)

Fyysisen turvallisuuden suunnittelussa on tarpeen mukaan otettava huomioon myös elektronisen ja muun tiedustelun mahdollisuus. Viranomaistasolla suojauksilta edellytetään, että ikkunoissa on näköesteet joiden tehtävä on peittää suora näkyvyys tilaan turva-alueen ulkopuolelta. Elinkeinoelämän suosituksena eli vähimmäistasona pidetään sitä, ettei ikkunoita saa rikkomatta auki ulkopuolelta. Ulkopuolelle kuulumattomien langattomien verkkojen kuuluvuus esimerkiksi kaikille avoimiin parkkialueisiin on hyvä estää, mikäli tämä on mahdollista. Elinkeinoelämässä tällaista elektronista suojausta ei kuitenkaan pidetä välttämättömänä. Tiloissa sisällä on rakenteissa toteutettava riittävä äänieristys etteivät tiloissa käydyt keskustelut kuulu ulkopuolisille. (Puolustusministeriö 2011, 61-65).

Fyysinen turvallisuus on osittain myös lainsäädännön tasolla säänneltyä. Aiheeseen liittyviä säännöksiä on muun muassa työturvallisuuslaissa, pelastuslaissa, arkistolaissa ja laissa yksityisyyden suojasta työelämässä. Lisäksi viestintäviraston teletoimintamääräyksissä on otettu kantaa fyysisen turvallisuuden asioihin. (Andreasson & Koivisto 2013, 52.)

4.3 Henkilöstöturvallisuus

Henkilöstöturvallisuus käsittää tietojärjestelmien käyttäjien toimintakyvyn ylläpitämiseen liittyvät toimenpiteet sekä näiden käyttäjien käyttöoikeuksien rajaamiseen liittyvät asiat. Tietojärjestelmät eivät järkevästi suunnittelussa ympäristössä ole kaikille avoimia, ja pienissäkin yrityksissä on usein tarkoituksenmukaista pitää osa tiedoista, kuten työsopimukset ja yrityksen taloudenpitoon liittyvät asiat, ainoastaan yrityksen johdon käsissä vaikka luottamus työntekijöihin olisikin kunnossa. Henkilöstöturvallisuuden osa-alueeseen kuuluvat erilaiset varamiesjärjestelyt, koulutuksen ylläpitäminen, tietojärjestelmiä koskevien vastuiden ja oikeuksien määrittelyt sekä joissakin tapauksissa rekrytointiprosessiin liittyvä turvallisuusselvitys tai rikosrekisteriotteen tarkastaminen. Jos yrityksen toiminnan kannalta kriittiset järjestelmät ovat vain yhden henkilön käytössä, liittyy näissä järjestelmissä olevien tietojen saatavuuteen järjestelmänkäyttäjään kohdistuva riski. Mikäli järjestelmän käyttäjä irtisanoutuu, kuolee tai sairastuu vakavasti, on kyseessä myös yritystoimintaa haittaava tietoturvallisuusriski. (Hakala ym. 2006, 11.)

Henkilöstöriskeihin kuuluvat myös henkilöstön rekrytoimiseen ja toimittajasopimuksiin liittyvät riskit, jotka ovat yrityksen sisäisiä henkilöstöriskejä. Rekrytoinnissa tärkeänä osana on taustatarkastuksen tekeminen rekrytoitavalle henkilölle, jolla voidaan vähentää vieraan henkilön palkkaamiseen liittyviä riskejä. Sama pätee myös uuteen yhteistyökumppaniin, jolla voi olla pääsy yrityksen suojattavaan tietopääomaan. Kauppakamarin tekemän tarkistuksen mukaan vuonna 2005 taustatarkistusten tekeminen ei kuitenkaan ole yleistä minkään kokoisissa yrityksissä. Kaikista suomalaisyrityksistä hieman yli kolmannes tekee rekrytointitilanteissa työnhakijasta jonkinlaisen taustaselvityksen. Väärän henkilön palkkaamisesta saattaa aiheutua merkittäviäkin tietoturvariskejä, esimerkiksi varkauksien tai sabotaasin muodossa. (Laaksonen ym. 2006, 139.)

Taustatarkistuksen voi toteuttaa yksinkertaisesti käymällä läpi työnhakijan ansioluettelossa mainittuja työnantajia ja varmistaa, että ansioluettelossa annetut tiedot pitävät paikkansa. Tämän lisäksi työntekijältä itseltään on hyvä pyytää työtodistukset näistä työpaikosta. Itse tehdyn taustaselvityksen lisäksi voidaan teettää luottotietojen ja rikostaustan selvittäminen. Turvallisuusselvityksen voi teettää suojelupoliisilla, mikäli työntekijällä on pääsy erityisen arvokkaisiin liike- tai ammattisalaisuuksiin tai näihin rinnastettaviin yksityisiin tietoihin tai omaisuuteen. Tällaisen selvityksen laajuudeksi riittää tavallisissa yrityksissä suppea turvallisuusselvitys. Turvallisuusselvitystä ei voi saada sellaiselle työnhakijalle, jonka työtehtävien ei katsota edellyttävän turvallisuusselvityksen teettämistä. Turvallisuusselvityksen teettäminen edellyttää työnhakijan antamaa lupaa. (Laaksonen ym. 2006, 140.)

Työnhakijan luottotiedot voidaan selvittää silloin, kun työnhakija olisi työtehtävissään välittömässä taloudellisessa vastuussa tai silloin, kun työtehtävä vaatii erityistä luottamusta työn-

tekijää kohtaan. Yksityishenkilöllä on oikeus saada tietää, kuka heidän luottotietojaan on kysellyt ja mihin tarkoitukseen. Luottotietoja kyseltäessä kyselyn tarkoitus on ilmoitettava. Keskuskauppakamarin mukaan luottotietojen selvittäminen on yleisempää kuin varsinainen taustaselvitys, hieman yli puolet suomalaisista yrityksistä ilmoittaa tarkistaneensa yhteistyökumppaneidensa luottotietoja. Suurissa yrityksissä tämä on yleisempää kuin pienissä tai keskisuurissa yrityksissä. (Laaksonen ym. 2006, 141.)

Työsuhteen irtisanominen muodostaa myös henkilöstöriskin, sillä työntekijöillä on usein hallussaan paljon hiljaista yrityksen toimintaan ja asiakassuhteisiin liittyvää tietoa. Tätä tietoa kulkeutuu muihin yrityksiin työntekijän mukana, sillä työntekijät vaihtavat usein työpaikkaa saman alan sisällä. On myös mahdollista, että kilpaileva yritys rekrytoi entisen työntekijän päästäkseen käsiksi tämän mukanaan tuomiin tietoihin omasta yrityksestä. Lainsäädäntö kieltää työntekijää ilmaisemasta liikesalaisuuden piiriin kuuluvia tietoja kilpailijalle, mutta epäeettistä ja laitonta toimintaa esiintyy myös yritysmaailmassa. Työntekijöiden käsittelemän tiedon rajaaminen hallitsee tätä riskiä. Työntekijän irtisanoutuessa esimiehen on harkittava, mitä tietoa yrityksen työntekijä saattaa viedä mukanaan ja mitä seurauksia voisi olla siitä, että tämä tieto kulkeutuu ulkopuolisten haltuun. Esimiehen on myös laadittava suunnitelma työntekijän tiedostojen käsittelyyn siten, että työnteko voi jatkua keskeytyksettä. Irtisanoutumisesta tulee myös tiedottaa muulle organisaatiolle ja varmistaa, että muut työntekijät ovat tietoisia siitä, ettei irtisanoutumisen kohteena oleva henkilö ole enää yrityksen palveluksessa. (Laaksonen ym. 2006, 144-145.)

4.4 Laitteisto- ja tietoliikenneturvallisuus

Laitteiston turvaaminen on osa teknistä tietoturvallisuutta. Tietoverkkoa hallinnoivalla taholla on oltava tieto siitä, millä laitteilla on sallittu pääsy tietoverkkoon. Tätä tarkoitusta varten voidaan perustaa laiterekisteri, johon kirjataan tiedot sellaisista laitteista, joilla on sallittu pääsy tietoverkkoon. Rekisteriin kirjataan myös hävitetyt ja käytöstä poistetut laitteet. (Puolustusministeriö 2011, 92.)

Teknisen tietoturvallisuuden toteuttamisen tärkeä tehtävä on salasanojen ja etähallittavien järjestelmien kirjautumisen turvaaminen. Pääkäyttäjän salasanaa tulee suojata hyvin, ja tarvittaessa järjestelmien kirjautumista pitää rajoittaa siten, ettei pääkäyttäjätunnuksella voi kirjautua tietoverkkojen ylitse vaan kirjautumisen on tapahduttava paikan päältä. Käyttäjien salasanat on myös suojattava. Järjestelmään voidaan määritellä vaadittava salasanan vähimmäistaso ja käyttäjien salasanoja voidaan testata käyttämällä samoja menetelmiä joita kyberrikolliset käyttävät salasanojen murtamiseen. Mikäli joukosta löytyy helposti murrettavia salasanoja, on nämä vaihdettava. Yksilölliset, vahvat ja määräajoin vaihdettavat salasanat rajaavat tehokkaasti ulkopuoliset tunkeutujat ulos järjestelmistä. Salasanojen tietoturvaa

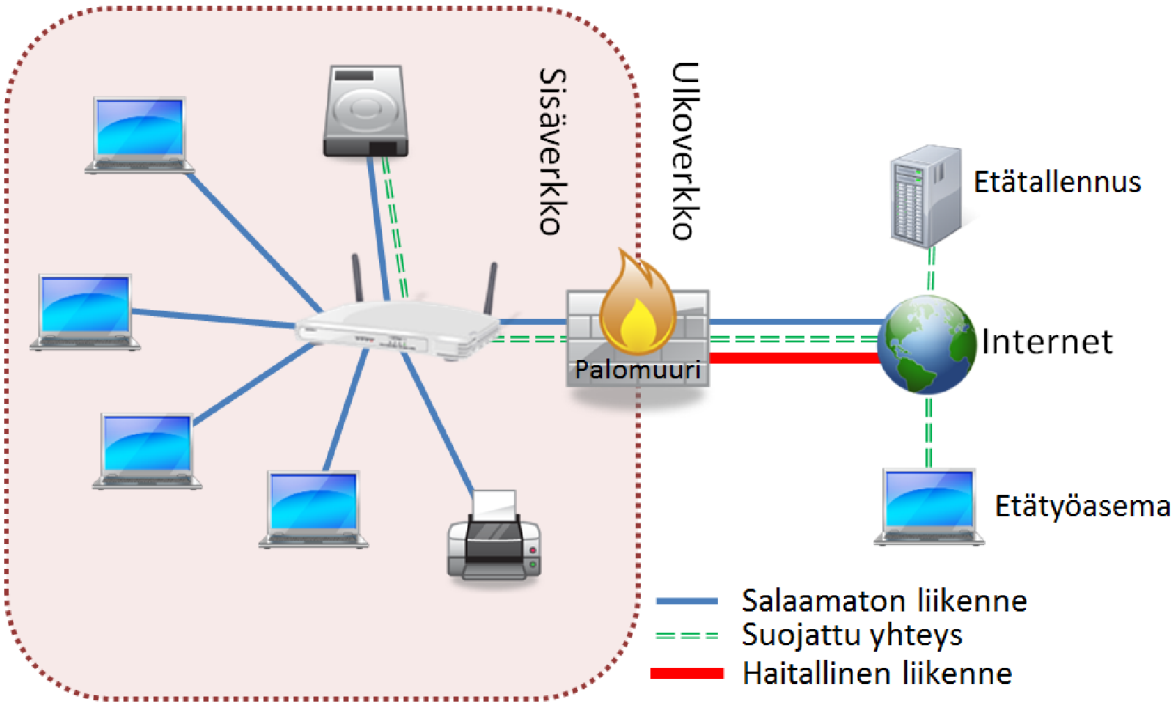
varmistettaessa on otettava huomioon, että salasanakin on henkilötietolain mukainen henkilötieto, ja salasanojen testaamisesta on sovittava yhdessä henkilöstön kanssa. Skannauksen tuloksena löydetyt heikot salasanat ilmoitetaan käyttäjälle ja käyttäjä itse vaihtaa tilalle vahvemman salasanan. (Laaksonen ym. 2006, 178-180.)

Tietoverkkojen tekniseen suojaamiseen on lähes rajaton määrä työkaluja ja ohjeita. Valittavat ratkaisut riippuvat niin tietoverkon rakenteesta kuin käytettävistä resursseista ja halutusta suojaamisen tasostakin. Lähtökohtana voidaan kuitenkin pitää sitä, että tietoverkko on suunniteltu loogisesti, siihen on pääsy vain yrityksen erikseen hyväksymillä henkilöillä ja että se on rajattu ulkoisesta Internetistä palomuurilla. Palomuuri rajaa sisäverkon ja ulkoverkon välisen liikenteen siten, että vain sallittu liikenne päästetään läpi. Verkko voidaan jakaa myös tietoturvavaatimuksiltaan eritasoisiin osiin, ja ohjata näiden verkkojen läpi kulkeva liikenne oman palomuurinsa kautta liikenteen edelleen rajaamiseksi. Yrityksen sisäverkko voidaan rajattava vierailijoiden käyttöön varatusta langattomasta verkosta siten, ettei liikenne kulje samassa verkossa laisinkaan. Liittymäpisteet yrityksen sisäverkkoon, kuten kytkimet, tulee suojata fyysisen turvallisuuden keinoin. (Laaksonen ym. 2006, 181-190.)

Yritysverkkoa suojaavan palomuuri vähimmäistasona voidaan pitää tasoa, joka rajoittaa kaiken muun paitsi yrityksen käyttämien laitteiden ja ohjelmistojen toiminnan kannalta pakollisen liikenteen pois verkosta. Estetystä liikenteestä kirjataan lokitieto, johon pyritään kirjaamaan tarkat tiedot liikenteen lähde- ja kohdeosoitteista. Lisäksi yleisiin verkkohyökkäyksiin on varauduttu riittävin teknisin ratkaisuin. (Puolustusministeriö 2011, 77.)

Kuviossa 5 on tyypillinen yritysverkko, joka on suojattu palomuurilla ja jossa yhteys yrityksen verkon sisällä oleviin palveluihin otetaan salatun yhteyden avulla. Yrityksen sisäverkon sisäpuolella olevat tietokoneet saavat viestiä toisilleen sekä verkkolevylle salaamattomilla yhteyksillä. Etätallennusjärjestelmä sijaitsee kolmannen osapuolen palvelimella, johon varmuuskopioidaan yrityksen verkkolevyn sisältö. Yhteys etätallennusjärjestelmään on salattu. Haitallinen ja ei-toivottu verkkoliikenne pysähtyy sisä- ja ulkoverkon reunalle asetettavaan palomuuriin.

Kuvio 5: Yrityksen lähiverkon suojattu verkkoliikenne



Palomuuriin voidaan tehdä etäyhteyden mahdollistavat liikennöintisäännöt. Moderneilla salausmenetelmillä on mahdollista antaa yrityksen sisäverkon turvallinen käyttöoikeus myös etätyöntekijöille niin sanottujen VPN (Virtual Private Networking)-yhteyksien avulla. VPN luo salatun yhteyden julkisen internetin ylitse yrityksen sisäverkkoon, jolloin etätyöntekijällä on pääsy esimerkiksi tietokantoihin tai verkkolevylle. Salausmenetelmiä voi käyttää myös yritykselle kriittisen tiedon suojaamisessa, ulkoisten massamuistien suojaamisessa, kannettavien tietokoneiden muistivälineiden salaamisessa ja työpöytäkoneiden kovalevyjen salaamisessa. Tämä vähentää riskiä tietojen vääriin käsiin joutumisesta vaikka työntekijän työvälineet varastettaisiinkin. (Laaksonen ym. 2006, 195-196.)

4.5 Ohjelmistoturvallisuus

Ohjelmistoturvallisuuden ulottuvuus käsittelee yrityksen toiminnassa käytettäviin ohjelmistoihin liittyviä riskejä. Ohjelmistoturvallisuuteen liittyvät mm. ohjelmistoissa olevat tietoturva-aukot, jotka voivat altistaa tietoturvaloukkauksille, ohjelmistojen virheelliseen toimintaan tai käyttöön liittyvät riskit jotka voivat johtaa tietoturvallisuuden sisäisen riskin toteutumiseen laiterikon muodossa, hankittujen ohjelmistojen sopivuus käyttötarkoitukseensa sekä ohjelmistojen toiminnan virheettömyys ja luotettavuus. (Hakala ym. 2006, 11-12.)

Ohjelmistoturvallisuuden osalta riskienhallinta edellyttää, että yritystoiminnassa käytetään ajantasaisia työkaluja. Yrityksen tietoturvasta vastaava taho ei itse pysty varmistamaan ohjelmistojensa turvallisuutta muuten kuin pitämällä ne päivitettyinä ja tarkkailemalla aktiivisesti tuotantokäytössä olevien ohjelmistojen julkaistuja tietoturvariskejä. Ohjelmistoturvallisuuden hallinnan kannalta on tärkeää käyttää ajantasaisia versioita ohjelmistoista ja käyttöjärjestelmistä ja varmistaa, että haittaohjelmien ja virusten torjunta on käytössä kaikissa työasemissa, joihin tuodaan tietoa järjestelmän ulkopuolelta verkosta tai muilla tallennusvälineillä. Virustorjunta perustuu tunnistetietokantaan, joten sitä on pidettävä aktiivisesti ajan tasalla. Modernit virustorjuntaohjelmistot päivittävät virustietokantansa internetin avulla, joten oikein asennettu virustorjunta on lisenssihuoltoa lukuun ottamatta huoltovapaa. (Hakala ym. 2006, 135-136.)

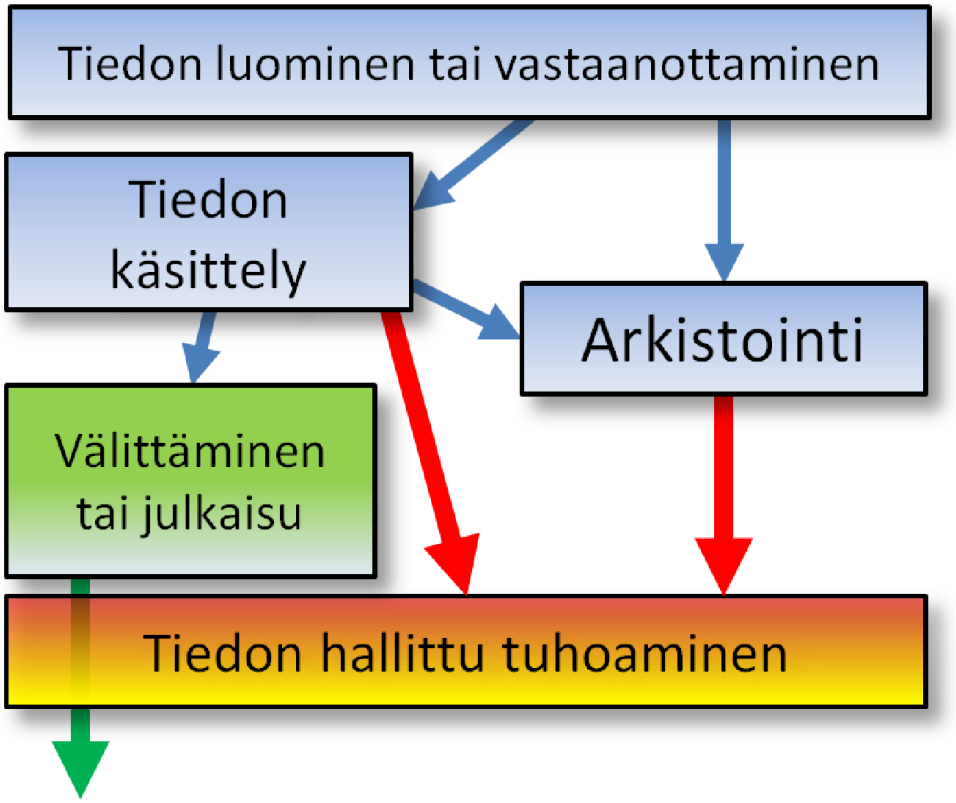
Haittaohjelmantorjunta on asennettava kaikkiin yrityksen verkossa oleviin ja siihen ulkoverkon kautta kytkeytyviin laitteisiin. Torjuntaohjelmistojen on oltava toimintakykyisiä ja käynnissä aina, kun laitetta käytetään. Torjuntaohjelmistojen lokitiedot on kerättävä talteen ja käyttäjiä on ohjeistettu haittaohjelmauhasta ja tietoturvaperiaatteiden mukaisesta toiminnasta tilanteissa, joissa haittaohjelmatartuntaa epäillään. Haittaohjelmahavaintojen aktiivinen seuraaminen on myös tärkeää. (Puolustusministeriö 2011, 87.)

Virustorjunta ei kuitenkaan suojaa ohjelmistoissa ilmeneviltä tietoturva-aukoilta. Ohjelmistojen valmistajat kuitenkin päivittävät aktiivisesti tuotannossa olevien ohjelmistojen tietoturvaominaisuuksia ja korjaavat niistä löytyneitä haavoittuvuuksia. Tämän vuoksi ajantasaisten versioiden ylläpitäminen on tärkeää. (Hakala ym. 2006, 135.)

4.6 Tietoaineistoturvallisuus

Tietoaineistoturvallisuuteen liittyy tietojen koko elinkaareen aikainen turvallinen käsittely. Tietoaineistoturvallisuuteen liittyvät kysymykset liittyvät tiedon säilyttämiseen ja arkistoimiseen, varmistamiseen, palauttamiseen sekä tuhoamiseen liittyvät toimenpiteet. Tietoaineistoturvallisuus tarkoittaa sitä, että tietoaineistojen käsittelyssä ylläpidetään yleisiä tietoturvallisia menettelytapoja. Tietoaineistoturvallisuuteen liittyvät tekniset ratkaisut kuuluvat muiden tietoturvallisuuden osa-alueiden alaisuuteen (Hakala ym. 2006, 11.) Kuviossa 6 on kuvattu esimerkki tiedon hallitusta käsittelystä organisaation sisällä sen luomisesta tai vastaanottamisesta sen tuhoamiseen asti. Myös arkistoitava tieto tuhotaan yleensä joskus.

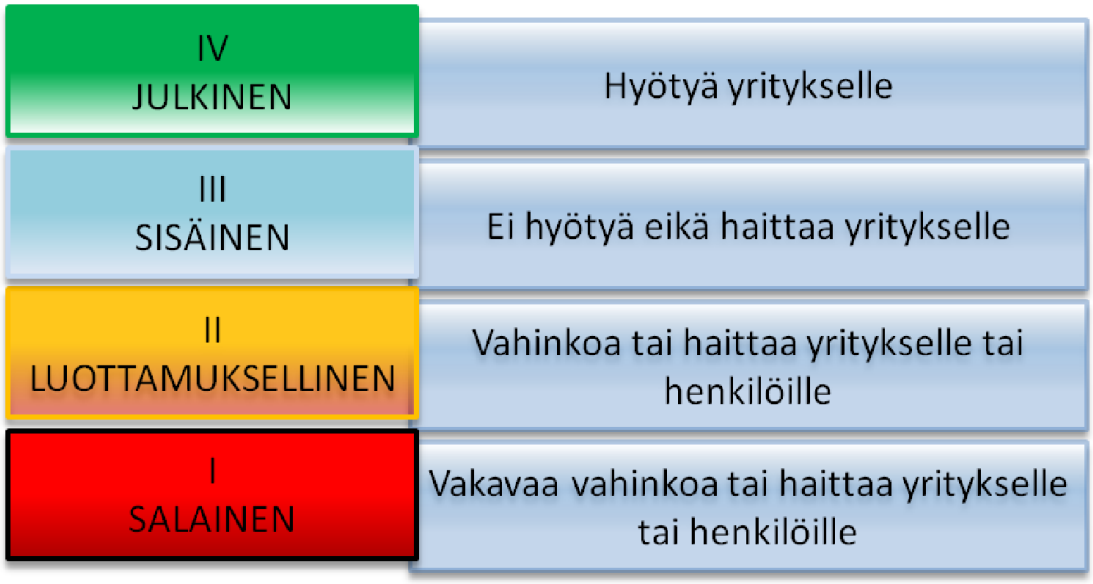
Kuvio 6: Hallittu tietoaineiston käsittelyn elinkaari



Varmistamattoman liikuteltavat tallennusalustat kuten USB-muistitikut tai ulkoiset kovalevyt tuottavat hallitsemattomana suuren riskin. Tämä riski tulee hallita järjestämällä liikuteltaville tallennusmedioille salakirjoitusjärjestelmä ja käyttämällä yrityksen koneissa ainoastaan hyväksyttyjä tallennusvälineitä. Liikuteltavaan mediaan liittyy aina katoamisriski, jolloin suurikin määrä yrityksen suojattavaa dataa saattaa joutua ulkopuolisten käsiin. Riskit korostuvat, mikäli tietoa siirretään yrityksessä toimipaikasta toiseen liikuteltavilla medioilla esimerkiksi postitse tai muuten sellaisella tavalla, että media voi kadota. Tiedon turvallinen siirtäminen on suunniteltava ja toteutettava siten, että tämä riski saadaan hallittua. (Layton 2007, 65.)

Tietojen sisäinen luokittelu julkiseen, sisäiseen, luottamukselliseen ja salaiseen on hyvä tapa tietoaineiston turvallisen käsittelyn ohjaamiseen. (Laaksonen 2006, 156-157.) Kuviossa 7 on kuvattu tämänkaltainen, neliportainen dokumenttiluokittelumalli jossa dokumenttien turvallisuusluokittelu määritellään neliportaisesti niiden paljastumisesta seuraavien vaikutusten perusteella.

Kuvio 7: Asiakirjojen luokittelu yrityksessä



Tietojen sisältö määrittelee niiden suojaamisen tarpeen, ja tietojen luokittelu auttaa suojausjärjestelmien oikeanlaiseen suunnitteluun ja kohdentamiseen. Tietojen luokittelusta on myös hyötyä, kun suunnitellaan niiden käsittelyyn tarkoitettujen laiteympäristöjen toteuttamista ja virhetilanteista toipumista. Luokkien perustana on oltava määritellyt sisältökriteerit, joiden perusteella tiedot osataan ohjata oikeaan luokkaan. Neljään kategoriaan perustuva luokittelusääntö on hyvä ja selkeä perussääntö, jonka avulla tietojen luokittelu ei muutu liian vaivalloiseksi. Toimisto-ohjelmat voidaan asentaa siten, että ne edellyttävät luotavien dokumenttien määrittelemistä johonkin tietoturvaluokkaan, jolloin luokittelemattoman tiedon määrä vähenee. (Laaksonen ym. 2006, 156-157.) Tietoaineiston turvallisuuden kannalta pääsyä eri aineistoihin on valvottava käyttöoikeusmäärittelyillä (Puolustusministeriö 2011, 89).

Tietojen suojaamisessa on varmistettava myös lakisääteiset velvollisuudet. Dokumentit on merkittävä niiden suojaustasoa kuvaavalla merkinnällä, ja useasta dokumentista koostuvaa kokonaisuutta, joka sisältää eri luokkiin kuuluvia osia merkitään ylintä suojaustasoa kuvaavalla merkinnällä. Mikäli pääasiakirjan ja sen osien luokitus ei ole sama, tämän on hyvä käydä ilmi dokumentista. (Puolustusministeriö 2011, 99.)

5 Opinnäytetyöprosessin kuvaus

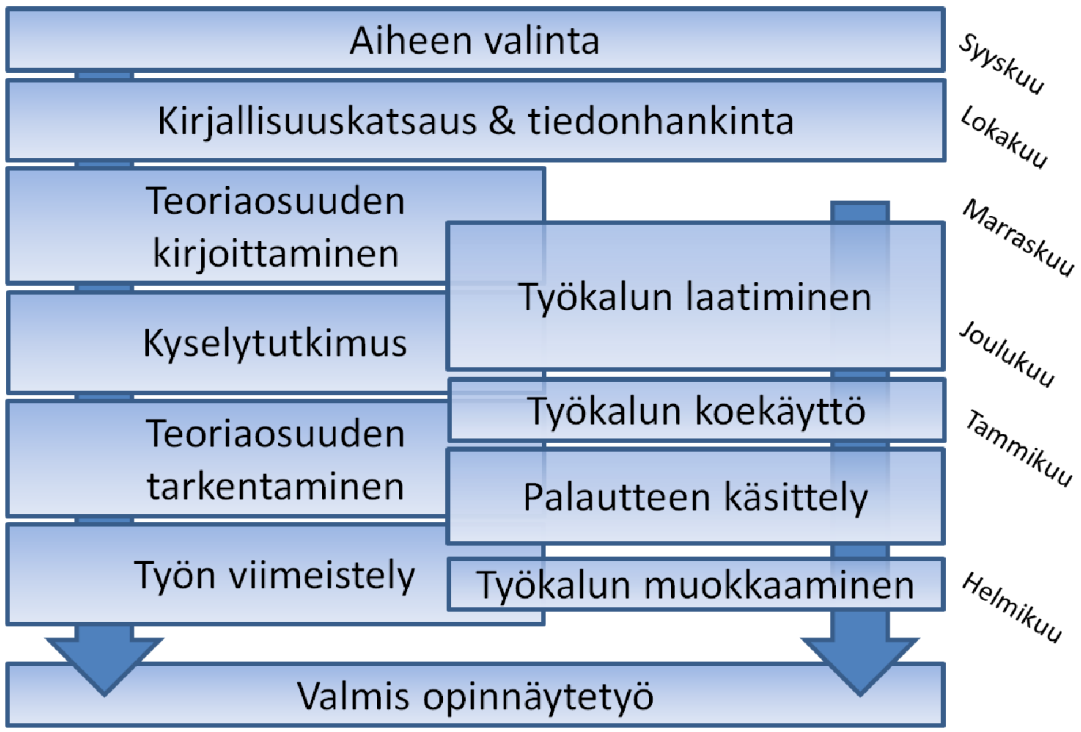
Opinnäytetyön tekeminen alkoi syksyllä 2013 aiheen hahmottelulla. Aiheen valintaan vaikutti vahvasti senhetkinen työni vanhempana rikoskonstaapelina Helsingin poliisilaitoksessa. Työssäni kohtasin runsaasti pienten yritysten edustajia, jotka olivat joutuneet tietotekniikkarikoksen uhreiksi. Nämä rikokset kohdistuivat yritysten tiedolliseen pääomaan. Suurimman osan

näistä rikoksista olisi voinut estää tekemällä edes jonkinlaista perustyötä tietoturvallisuusriskien hallinnan eteen. Samat laiminlyönnit, kuten salasanahallinnan surkea taso, toistuivat aina, ja niiden taustalla tuntui aina olevan joko puutteellinen tietoturvatietoisuus tai välinpitämättömyys tietoturvakysymyksiä kohtaan.

Päätin tehdä toiminnallisena opinnäytetyönä jonkinlaisen oppaan tai työkalun, jonka avulla pienten yritysten omistajat tai työntekijät voivat välttää tilanteen, jossa tietoturvallisuuden riskeihin herätään vasta jo tapahtuneen vahingon jälkeen. Halusin laatia työkalusta helposti lähestyttävän ja käytettävän.

Työn tutkimuksellisiksi menetelmiksi valitsin kirjallisuuskatsauksen ja asiantuntijoille suunnatun kyselyn. Näiden menetelmien lisäksi pyysin muutamaa koekäyttäjää käyttämään lähes valmista työkalua ja kertomaan minulle kokemuksistaan. Sain opinnäytetyön valmiiksi helmikuussa 2014. Opinnäytetyön tekemisen osa-alueet aikatauluineen on esitetty kuviossa 8.

Kuvio 8: Opinnäytetyön tekemisen vaiheet



Opinnäytetyötä ja siihen liittyvää työkalua hion ja muokkasin runsaasti tammi-helmikuussa. Kokonaisuudessaan opinnäytetyön tekemiseen meni minulta noin viisi kuukautta. Olin koko tämän ajan päivätyössä, joten työn tekeminen ajoittui pääsääntöisesti viikonloppuihin ja iltoihin.

5.1 Tiedonhankinnan menetelmät

Työkalun laatimista varten piti hahmottaa vastaus työn keskeiselle tutkimuskysymykselle: mitkä keskeiset, virheelliset käytännöt tai politiikat altistavat pieniä yrityksiä tietoturvaloukkauksille ja -häiriöille? Tietoturvallisuuden hallinnasta on kirjoitettu paljon hyviä kirjoja, joissa toistui selkeästi samoja teemoja joiden perusteella pystyin hahmottamaan työlleni selkeän jaottelun. Valikoin katsaukseen alan peruskirjallisuutta, KATAKRI II-ohjeita sekä eri viranomaisten verkossa julkaisemia ohjeita.

Kirjallisuuskatsaukseen kuuluva tiedonhaku tarinankerronnan teoriasta vei minut vieraalle maaperälle, sillä aihe tuntuu mielestäni kuuluvan enemmän sosiaalitieteisiin kuin turvallisuusalalle. Aiheeseen tutustuminen oli kuitenkin mielenkiintoista, ja huomasin, että omassakin ajattelussani on runsaasti urautumista, josta on hyvä pyrkiä eroon. Tarinankerronnan käyttäminen koulutuksen menetelmänä on runsaasti tutkittu aihe, ja aion käyttää sitä jatkossa itse pääasiallisena tapana esittää tapauksia esityksissä ja koulutustilanteissa.

Kirjallisuudesta on haettu teoreettinen tausta sille, mitä asioita ylipäänsä tietoturvallisuuden käsitteen alle kuuluu ja mistä puhutaan, kun puhutaan yritysten tietoturvallisuudesta. Halusin näiden asioiden lisäksi selvittää alan asiantuntijoilta ”kentällä” tehtyjä havaintoja siitä, mikä arkielämän tilanne tietoturvallisuustyön osalta yrityksissä on.

Kyselytutkimuksen tein joulukuussa 2013, jonka tuloksien perusteella teemoittelin yleisimpiä tietoturvallisuutta uhkaavia asioita. Kyselytutkimusta kohteeksi valitsiin poliisin tietotekniikkarikostutkijat ja tietotekniikkarikosten avainsyyttäjät, jotka osallistuivat vuoden 2013 tietotekniikkarikostutkinnan seminaariin Parolassa. Kyselylomake lähetettiin sähköpostitse yhteensä 49 henkilölle. Vastauksia kyselyyn sain vain yhdeksän kahdesta lisävastauspyynnöstä huolimatta. Saamani vastaukset olivat kuitenkin laadukkaita, joten sain niistä mielestäni riittävästi materiaalia muita tutkimuksellisia menetelmiä tukemaan. Työkokemusta tietotekniikkarikostutkinnan alalta vastaajilla oli keskimäärin 18,4 vuotta, joten kokemuksen tuoma asiantuntijuus vastaajien keskuudessa on merkittävä.

Asiantuntijakyselyssä esille nousseiden teemojen ja kirjallisuuden perusteella laadin tammikuussa tietoturvallisuusloukkaustapauksista kertovat tarinat, joista koostin varsinaisen työkalun sisällön. Työ valmistui lopulliseen muotoonsa helmikuussa.

Työkalun versio 1.0 lähetettiin kolmelle organisaatiolle koekäytettäväksi. Kaksi organisaatioista oli pieniä yrityksiä ja kolmas oli yleishyödyllinen, pääosin julkisrahoitteisesti toimiva rekisteröity yhdistys. Yhdistys valittiin mukaan sen selvittämiseksi, soveltuuko työkalu myös voittoa tavoittelemattomien organisaatioiden käyttöön. Koekäyttäjäorganisaatiot valitsin kysy-

mällä tuttava- ja perhepiiristäni yrittäjiä, jotka olisivat halukkaita käyttämään työkalua ja raportoimaan sen tuloksista. Lähetin työkalun sähköpostilla koehenkilöille. Työkalun yhteydessä olevassa sähköpostissa kysyttiin yrityksen kokoon ja liikevaihtoon liittyviä perustietoja, yrityksen laitekannan kokoa, käytössä olevien sähköisten järjestelmien määrää ja laatua sekä vastaajien käsityksiä tietoturvallisuudesta käsitteenä. Sähköpostissa kehotettiin käyttämään työkalua kysymysten välissä ja mittaamaan siihen kuluva aika.

Työkalun käyttämisen jälkeen kysyttiin, avasiko työkalu käsitystä tietoturvallisuuden piiriin kuuluvista riskeistä, tunnistettiinko työkalun avulla riskejä omassa yritystoiminnassa ja johtaako työkalun käyttäminen yrityksessä konkreettisiin muutoksiin. Työkalun koekäytön analysointivaiheessa yrityksiä käsitellään nimettöminä, sillä työkalun käyttäminen paljasti niissä selkeitä tietoturvallisuuspuutteita, eikä tämän työn tavoitteen kannalta ole tarkoituksenmukaista julkaista sellaista tietoa, jonka avulla haavoittuvia yrityksiä voi tunnistaa.

6 Asiantuntijakyselyn tulokset

Tässä työssä kyselytutkimusten vastaukset teemoitellaan. Teemoittelu on tiedon analysointimenetelmä, jolla etsitään teemoja, joiden alaisuuteen yksittäiset vastaukset voidaan luokitella. Teemoittelulla pyritään sellaisten yleisten ilmiöiden löytämiseen, joihin tämän opinnäytetyön tuloksena luotavalla työkalulla voitaisiin vaikuttaa. Vastaukset jaettiin kysymystyypin mukaan siten, että vapaat tekstivastaukset teemoiteltiin, ja pistevastauksista laskettiin keskiarvot. Asiantuntijoille lähetetty kyselylomake on kuvattu liitteessä 1.

6.1 Vapaiden vastausten teemoittelu

Aineiston vastauksia käsiteltäessä esille nousi selkeästi kaksi keskeistä teemaa, jotka toistuivat lähes kaikissa vastauksissa. Käytännössä muutamaa poikkeusta lukuun ottamatta kaikki vastaukset voitiin asettaa jommankumman teeman alle. Nämä teemat olivat välinpitämättömyys ja tietämättömyys.

Välinpitämättömyyttä kuvasivat vastaukset, joissa kerrottiin ohjeita olevan kyllä olemassa, mutta niiden noudattamisen olevan puutteellista. Joissakin vastauksissa kerrottiin, että olemassa olevista ohjeista luistetaan siksi, että jokin asia on helpompi tehdä ohjeita vastoin. Lisäksi välinpitämättömyyden yhtenä muotona oli ”sokea usko omaan tekniikkaan”. Eräs vastaus kuvasi hyvin tietoturvallisuuden suunnittelun ja toteutuksen välistä ongelmaa: ”paperit ovat usein kunnossa, käytännöt ovat vain toiset.” Tiedon käsittely tuntui olevan vastausten perusteella keskimäärin holtitonta ja jäsentymätöntä. Salaista materiaalia ei erotettu mitenkään julkisesta ja kaiken tiedon käsittelyssä oltiin huolimattomia ja löperöitä. Tietoturvaan

suhtauduttiin niin kuin sitä ei tarvitsisi ajatella laisinkaan. Tähän teemaan kuuluvia vastauksia oli kaikissa kysymyslomakkeissa.

Toinen esille selkeästi noussut teema oli *tietämättömyys*. Tietämättömyys ilmeni siten, että tietoturvallisuuskoulutusta ei annettu ja tietoaineistoja käsiteltiin ”holtittomasti”. Omia välineitä sai työpaikalla käyttää kenenkään estämättä ja erilaisia tallennusvälineitä koskevia ohjeita ei ollut. Tässä heijastui vastauksissa se, että muun muassa omia tallennusvälineitä kuten USB-muistitikkuja sai käyttää ilman rajoituksia. Ilmeisesti tällaisiin välineisiin liittyvät virus- ja tietoturvariskit eivät ole organisaation tiedossa. Puuttuva ohjeistus tietoturvaloukkausten varalta nousi esille asiana, jota voidaan perustellusti pitää tietämättömyyteen perustuvana ongelmana. Eräs vastaaja kertoi, että ”tietoa ja koulutusta aletaan hankkia vasta, kun savu jo nousee.” Toinen vastaaja kertoi, että johdon osaamattomuus on yksi keskeinen syy tietoturvallisuustason heikkouteen. Tähänkin teemaan kuuluvia vastauksia oli kaikissa kyselylomakkeissa.

Tyypillisesti käytännöissä ja politiikoissa nousi esille ongelmia, jotka voitaisiin ratkaista hallinnollisen tason keinoin. Perusongelmat ovat vastausten perusteella niin korkealla tietoturvallisuuden osa-alueiden hierarkiassa, että yksittäisiä tapauksia tai käytäntöjä ei oikeastaan noussut esille ainuttakaan. Vastaajien antamien vastausten keskeinen sisältö oli se, että tietoturvallisuus jätetään ylipäänsä huomiotta. Tästä johtuen kyselytutkimuksen vastauksina saatuja asioita ei voitu sinänsä suoraan tuoda osaksi työkalun skenaarioita, mutta kyselytutkimuksen vastaukset kyllä vahvistavat sekä olemassa olevaa tarvetta Tikan kaltaiselle työkalulle että oletusta siitä, että tietoturvallisuusongelmien ratkaiseminen yrityksessä alkaa ongelman olemassaolon tunnistamisella.

Vastaajia pyydettiin listaamaan kolme yleisintä asiaa, käytäntöä tai politiikkaa jotka altistavat yrityksen tietoturvaloukkauksille. Vastauksissa oli eritelty yleisellä tasolla ilmiöitä, ja näissäkin vastauksissa vastaukset pystyi asettamaan sekä tietämättömyyden että välinpitämättömyyden teemojen alaisuuteen. Oikeastaan seuraavaan lainaukseen voidaan tiivistää kaikissa vastauksissa näkyvä yleinen sävy: ”henkilöstön tietämättömyys, taitamattomuus, huolimattomuus ja välinpitämättömyys sekä koulutuksen puute.”

6.2 Tietoturvallisuustoiminnan eri osa-alueiden pisteytys

Kysymyslomakkeen osa-alueiksi valittiin operatiivista toimintaa kuvaavia osa-alueita. Esimerkiksi tietoturvallisuuskoulutus-, ohjeistus ja –tietoisuus jaettiin kolmeen eri osa-alueeseen, vaikka kaikki osa-alueet kuuluvat sinänsä hallinnollisen turvallisuuden kokonaisuuden alaisuuteen. Kyselyllä haluttiin mitata sekä yritysten tahtotilaa että käytännön toteutusta. Tämän

vuoksi ohjeistuksen ja koulutuksen lisäksi kysyttiin tietoturvatietoisuuden tasosta, joka kuvaa sitä miten hyvin koulutus ja ohjeistus on mennyt perille.

Kyselylomakkeessa oli käytetty sekä vapaalla tekstikentällä olevia kysymyksiä että järjestys-asteikkokysymystä jossa otettiin kantaa siihen, miten hyvin tietyt tietoturvallisuuden osa-alueet on yrityksissä keskimäärin hoidettu. Asteikon kysymyksenä on ”miten seuraavat asiat ovat oman arviosi mukaan keskimäärin yrityksissä, joiden asioita käsittelet?” Vastausskaalaksi annettiin ”1 = toteutettu erittäin huonosti - 5 = toteutettu erittäin hyvin.” Kysymys mukailee Likertin järjestysasteikon kysymysskaalaa, jossa kysytään suoraan mielipidettä valmiiseen väittämään asteikolla ”Täysin samaa mieltä” - ”Täysin eri mieltä” (KvantiMOTV 2007).

Taulukkoon 2 on koottu asteikkokysymysten osa-alueiden pisteiden keskiarvot. Tämän jälkeen osa-alueet on järjestetty parhaat pisteet saaneesta huonoimmat pisteet saaneeseen ja näin laskettu kaikkien osa-alueiden keskipisteet yhden yleispistemäärän saamiseksi. Yleispistemäärä kuvaa sitä, miten kaikkien osa-alueiden toteutus on koko kyselyn keskiarvon mukaan hoidettu.

Taulukko 1: Tietoturvallisuutta koskevien toimintojen pistekeskiarvot

Osa-alue	Pisteet
Toimitilaturvallisuus	3,22
Tietoturvallisuuskoulutus	3,00
Paperitulosteiden käsittely	2,67
Salasanahallinta	2,56
Tietoturvallisuustietoisuus	2,44
Tietoturvallisuusohjeistus	2,22
Tietoverkkoturvallisuus	2,11
Tietoturvallisuuskoulutus	2,00
Tietojen ja dokumenttien turvallisuusluokittelu	2,00
Mobiililaitteiden tietoturvallisuus	1,89
Kaikkien osa-alueiden keskiarvo	2,41

Kaikkien osa-alueiden saamien pistekeskiarvojen keskiarvo oli 2,41 pistettä kyselyn “ei hyvin eikä huonosti”-keskiarvon ollessa 3. Kyselyn perusteella asiantuntijoiden yleinen näkemys oli

se, että tietoturvallisuuteen liittyvät asiat on yleensä hoidettu keskiarvoa huonommin. Toimitilaturvallisuus arvioitiin hoidetuksi hieman keskiarvoa paremmin. Taulukosta voidaan nähdä, että mobiililaitteiden tietoturvallisuus on hoidettu keskimäärin kaikista heikoimmin.

7 Tikka-kartoitustyökalu

Tämän opinnäytetyön tuloksena laadittava Tikka-kartoitustyökalu on tarkoitettu ensisijaisesti sellaisten pienten yritysten käyttöön, joissa tietoturvallisuustoiminta on vielä suunnittelematonta ja johtamatonta. Työkalusta saa parhaan mahdollisen hyödyn silloin, kun se on yrityksen ”ensikosketus” tietoturvallisuuteen liittyvien riskien tunnistamiseen ja havainnointiin. Sen on tarkoitus luoda sen käyttäjässä heräte suunnittelemaan ja pohtimaan oman yrityksen tietoturvatilannetta kuuden, tosielämän tapauksiin perustuvan tarinan avulla. Työkalua ei suunniteltu sellaiseksi, että sen avulla voidaan suoraan saattaa yritysten tietoturvallisuustoiminta hyväksyttävälle tasolle, vaan sen on tarkoitus toimia yrityksen tietoturvallisuustyön alkuun panevana voimana. Työkalun lopussa tarjotaan viitteitä lähteisiin, kuten Puolustusministeriön kansalliseen turvallisuusauditointikriteeristö KATAKRIin, Viestintäviraston tietoturvaoppaaseen ja Valtionvarainministeriön VAHTI-tietoturvaohjeisiin, joiden avulla yrityksen varsinainen tietoturvallisuustyö voidaan aloittaa.

Arvelin, että perinteinen, taulukkomaiseen rakenteeseen laadittu tarkistuslistatyökalu ei juurikaan parantaisi tilannetta, sillä tämän kaltaisia työkaluja on jo runsaasti tarjolla. Ne ovat hyviä välineitä silloin, kun tietoturvallisuustyö on jo päätetty aloittaa, mutta kriittinen kynnys tuntuikin olevan tietoturvallisuustyön alullepano. Päädyin laatimaan työkalun, joka koostuisi tarinoista, joissa tietoturvallisuus pettää. Toivoin voivani tuoda tarinoiden avulla tietoturvallisuuden pettämiseen liittyvät ongelmat selkeästi ymmärrettäviksi ja hahmotettaviksi.

Työkalun avulla pyritään herättämään yrittäjä mieltämään tietoturvallisuusriskit kaikkea yritystoimintaa koskeviksi tosiasioiksi ja pahimmillaan vakavia seurauksia aiheuttaviksi riskeiksi. Tietoisuus riskeistä on toimivan riskienhallinnan ensimmäinen askel. Työkalun tavoitteena on, että yrittäjä aloittaa sen tekemisen jälkeen tiedonhaun tietoturvallisuuden toteuttamisesta yritysympäristössään ja tekee konkreettisia muutoksia yrityksessään. Lopullisena tavoitteena on toimiva, organisaation kulttuuriin ja toimintaan sopiva ja turvallinen tietojenkäsittelyympäristö.

Tikka-kartoitustyökalun kohderyhmänä ovatkin ihmiset, jotka eivät koe tietoturvallisuutta itselleen tutuksi aihepiiriksi. Työtä varten kirjoitetut tarinat ovat tyylinsä ja sisältönsä puolesta ns. case-kuvauksia ja niissä on piirteitä tosielämän tapahtumista.

Tiedonjakamisen ja koulutuksen menetelmänä tarina tarjoaa lukijalle mahdollisuuden myötäelää tarinan tapahtumia ja tätä kautta heijastella kertomuksen tapahtumia omaan yritystoimintaansa. Valitsin nimenomaan tarinat menetelmäksi myös siksi, että perinteinen ”rasti ruutuun”-taulukkotyökalu voi olla tietoturvallisuustyötä tekemättömälle myös työläs ja vaikeasti lähestyttävä, eikä se tarjoa tosielämään liittyviä esimerkkejä siitä, miksi asiat on syytä saattaa kuntoon. Halusin tarinoiden avulla tehdä työkalusta myös helposti lähestyttävän sekä viihdyttävän jotta kynnys sen käyttämiseen olisi mahdollisimman matala.

Nimi ”Tikka” on mukaileva lyhenne työkalun pitkästä nimestä, joka on ”tietoturvallisuustilanteen kartoitustyökalu pienille yrityksille.” Työkalun rakenteeksi valittiin tarinapohjainen kerronta. Tikkaan kuuluvat tarinat kertovat tosielämän esimerkeistä löyhästi lainaillen tapahtumista, joissa tietoturvallisuus pettää. Tikkaan kuuluvat tarinat perustan tapahtumiensa osalta omiin kokemuksiini tietotekniikkarikostutkijana.

Työkalun menetelmäksi valittiin case-pohjainen tarinankerronta, sillä tarinoiden kautta tekniset ja teoreettiset konseptit voidaan asettaa osaksi arkielämän kokemuksia. Tarinoiden tapahtumien kautta lukija voi pohtia, onko hänen organisaatiossaan tilanne sellainen että tarinassa kuvattu tapahtumaketju voisi osua oman yrityksen kohdalle. Tarinat tarjoavat lukijalle samaistumisen kokemuksia ja avaavat tietoturvallisuuteen liittyviä, joskus vaikeasti hahmotettavia käsitteitä. Tarinoiden lisäksi Tikka kertoo pienen yhteenvedon tarinan keskeisistä kohdista ja kysyy työkalun käyttäjältä kolme kysymystä yrityksen omasta tietoturvallisuudesta tarinan aihepiiristä. Kysymysten tarkoituksena on tiivistää tarinan olennaiset riskit kolmeen kysymykseen ja herättää työkalun käyttäjä vertaamaan tarinan tapahtumia omaan yritystoimintaansa.

8 Tikka-kartoitustyökalun koekäyttö

Tikka-kartoitustyökalu koekäytettiin kahdessa pienessä yrityksessä ja yhdessä yleishyödyllisessa yhdistyksessä. Koekäyttäjät käyttivät työkalua, jonka jälkeen he vastasivat siihen liittyviin saatekysymyksiin. Saatekysymyksissä kysyttiin mm. työkalun tekoon kulunutta aikaa, yrityksen kokoa, liikevaihtoa, vastaajien ennakkotietoja tietoturvallisuusasioista sekä yrityksen laitekantaa.

8.1 Koekäyttäjä A – Yksityisen sairaanhoitoalan yritys

Yritys A työllistää 51 henkeä, joten se ylittää yhdellä työntekijällä pienen yrityksen määritelmän rajan henkilöstönsä osalta. Tästä ei kuitenkaan aiheudu sellaista muutosta yrityksen toimintakulttuurille, että sillä olisi työkalun koekäytön kannalta merkitystä. Yrityksen liikevaihto on noin 1,5 miljoonaa euroa. Yrityksellä on 100 asiakasta. Yrityksessä on käytössä kahdeksan

tietokonetta, kuusi tablettia ja 14 matkapuhelinta. Yritys käyttää muutamia alakohtaisia erityisohjelmia ja tavanomaisia Windows-ympäristön varusohjelmia toimistotyöhön. Yrityksessä ei ole tehty kirjallisia ohjeita tai suunnitelmia tietoturvallisuudesta. Yritys käsittelee salassa pidettäviä tietoja, joista käsitellään lähinnä fyysisiä kopioita joita säilytetään turvallisesti.

Työkalua käytti yrityksen toimitusjohtaja. Työkalun käyttämiseen meni häneltä aikaa noin kymmenen minuuttia. Toimitusjohtaja kertoi työkalun avanneen hänen käsitystään tietoturvallisuusriskeistä merkittävästi. Toimitusjohtajalla oli hyvä ymmärrys tietoturvallisuuden käsitteestä sinänsä, mutta käsitteen merkitys oli hänen kuvailunsa mukaan suppea. Vastauksessa mainittiin lähinnä ohjelmisto-, laite- ja työasematurvallisuuden seikkoja. Toimitusjohtajan kertoman mukaan ”aikaa hukkaantui tuskanhien pyyhkimiseen otsalta” hänen tajutessaan, että kaikki tarinoiden vahingot voivat toteutua myös hänen yrityksessään. Yrityksessä oli tähän asti lähinnä ”seilattu tuurilla”, eli tietoturvallisuutta uhkaavilta riskeiltä oli kuitenkin vältytty. Toimitusjohtaja kuitenkin tunnisti, että kyseessä on todellinen, hallitsemista vaativa osa-alue yrityksen riskienhallinnassa. Hänellä oli tahtotila saattaa tietoturva-asiat yrityksessä kuntoon, mutta hän myös koki asian niin haastavaksi, ettei tätä voitu tehdä omin voimin. Toimitusjohtaja kertoi hankkivansa avuksi ulkopuolisen asiantuntijan. Toimitusjohtaja kertoi tunnistaneensa työkalun avulla omasta yrityksestään useita vakavia tietoturvariskejä ja että työkalun käyttäminen laajensi hänen käsitystään ylipäänsä tietoturvallisuuden piiriin kuuluvista asioista.

Käytännön toimiin tietoturvallisuuden kohentamisen osalta yrityksessä ryhdytään heti, kun jostain löydetään ulkopuolinen taho joka voi tarjota yritykselle sen tarvitsemia tietoturvapalveluita. Työkalu osoittautui yrityksessä hyödylliseksi.

8.2 Koekäyttäjä B – Yleishyödyllinen yhdistys

Yhdistyksessä on töissä 11 työntekijää ja sen liikevaihto on noin 600 000 euroa josta 450 000 euroa avustuksina ja loput oman varainhankinnan kautta. Yhdistyksellä on käytössään 16 tietokonetta ja 16 puhelinta. Yhdistyksessä on keskitetty dokumenttien hallinta, kalenterit ja sähköpostit pilvipalveluun, eikä siellä käytetä juurikaan erityisiä ohjelmistoja. Yhdistyksessä ei ole tehty kirjallisia ohjeita tai suunnitelmia tietoturvallisuudesta.

Työkalua käytti yhdistyksen hallintojohtaja, joka vastaa muun muassa yrityksen tietohallinnon ratkaisuista. Yhdistyksessä ei ole erityistä tietohallintotoimintaa. Yhdistys käyttää runsaasti pilvipalveluita, joissa yhdistyksen dokumenteista suurin osa on taltioitu. Pilvipalvelut tarjoavat keskitetyt kalenteripalvelut, dokumenttienhallinnan sekä sähköpostit kaikille työntekijöille. Hallintojohtajalla kului aikaa työkalun käyttämiseen muiden töiden ohessa noin runsas

tunti, mutta tähän aikaan sisältyi myös työkalun koekäytön haastatteluvastauksiin vastaaminen.

Hallintojohtaja kertoi, että tällä hetkellä varmuuskopiointikäytännöissä on hieman ongelmia. Niihin suunnitellut ratkaisut olivat jo kuitenkin vireillä. Yhdistyksessä on ratkaistu tiedon turvallisuusongelmat luottamalla vahvasti pilvipalveluihin, eikä paikallisesti toimitiloissa säilytetä juurikaan sellaista tietoa, joka kärsisi esimerkiksi varkaus- tai tulipalotapauksista. Tiedon palauttaminen eri lähteistä olisi kuitenkin työlästä, jonka vuoksi keskitettyä varmuuskopiointiratkaisua oltiin tuomassa käyttöön. Salasanahallinnassa tunnistettiin riskejä, joiden hallinnassa olisi parantamisen varaa.

Hallintojohtaja koki, että työkalu oli rakenteeltaan ja kieliasultaan selkeä. Mitään ”katastrofaalista ei tullut mieleen”, mutta hallintojohtaja totesi että merkittävä ongelma taitaa olla se, että ihmisillä on runsaasti ”hiljaista tietoa” jota ei ole kirjattu ylös mihinkään. Hallintojohtaja totesi myös olevansa ”itse yrityksen suurin tietoturvallisuusriski!” Hallintojohtaja kertoi, että ”ihmisten päissä olevia tietoja ja asioita ei ole dokumentoitu riittävästi, eli jos joku meistä jäisi kotimatkalla bussin alle, niin siinä katoaisi enemmän ”elintärkeää” tietotaitoa kuin yhdessäkään yksittäisessä [tieto]koneessa.” Tietoturvallisuusriskeistä tunnistettiin henkilöstöturvallisuuteen liittyviä tekijöitä, sillä yhdistyksen henkilöstöllä on runsaasti sellaista tiedollista pääomaa jota yhdistys tarvitsee mutta jota ei ole kirjattu mihinkään ylös. Tarinamuotoiset tapahtumakuvaukset saivat kiitosta. Työkalu koettiin ”herättelevänä”, ulkoasultaan luottamusta herättävänä ja käytännön esimerkkejä pidettiin hyvänä tapana tehdä tietoturvariskeistä helposti ymmärrettäviä. Työkalun alussa oleva alustusteksti sisälsi muutaman yksittäisen virkkeen, jotka eivät työkalun käyttäjän mielestä olleet tyylillisesti asianmukaisia, muun muassa maininta ”jälkiteollisesta yhteiskunnasta” koettiin ”korvaan särähtävänä”. Loppusanoja pidettiin hyvinä.

Yhdistyksessä ryhdytään työkalun käyttämisen jälkeen kirjaamaan tietoturvallisuuden toimintakäytäntöjä ylös, ja dokumentoimaan hiljaista tietoa. Hallintojohtaja myös halusi pitää työkalun itsellään ja käydä sen myöhemmin läpi vastauksineen uudelleen.

8.3 Koekäyttäjä C – Autokoulu

Yritys C työllistää neljä täysiaikaista ja kaksi osa-aikaista työntekijää. Asiakkaita yrityksellä oli vuonna 2013 noin 350 kappaletta. Vuoden 2013 liikevaihto oli noin 600.000 euroa. Yritys tarjoaa liikennekasvatuspalveluita. Käytössä on seitsemän tietokonetta, kuusi tablettia ja kahdeksan matkapuhelinta. Yrityksessä ei ole tehty kirjallisia ohjeita eikä suunnitelmia tietoturvallisuudesta.

Työkalua käyttivät yrityksen omistaja, joka toimii yrityksessä toimitusjohtajana, sekä ajo-opettaja, joka vastaa opetustyön lisäksi myös yrityksen käytännön toiminnasta. Yritys käyttää muutamia verkkopalveluja, joiden avulla ajokouluopetustoimintaa, aikataulutusta ja oppilaiden tietoja hallinnoidaan. Oppilaita koskeva tieto on kirjattu näihin järjestelmiin, joten yrityksen kannalta tärkeitä tietoja on keskitetty pääasiassa kolmannen osapuolen palveluihin. Yrityksen paikallisesti hallinnoimaa tietoa ovat pääasiassa asiakkaiden ja henkilökunnan käyttäjätunnukset ja salasanat yrityksen käyttämiin palveluihin. Salasanojen tai niitä sisältävien laitteiden katoamisen osalta on annettu suulliset ohjeet.

Yrityksessä on ollut tarkoitus laatia selkeät tietoturvallisuusohjeet jo pitkään. käyttäjillä on selkeä käsitys tietoturvallisuuden määritelmällisestä käsitteestä, ja tietoturvallisuus mielletiin laveasti tietojen suojaamiseksi ulkopuolisilta tai sisäisiltä väärinkäytöksiltä. Työkalussa ilmi tulevista riskeistä iso osa jo tiedostettiin, mutta niiden hallitsemiseen ei ollut vielä ryhdytty resurssien puutteen vuoksi. Työkalun käyttäjät kertoivat, että työkalu auttoi hahmottamaan tietoturvallisuuden eri osa-alueita ja helpottaa tällä tavoin kirjallisen tietoturvasuunnitelman laatimista. Lisäksi varmuuskopiointiratkaisuja aiotaan kehittää, sillä tällä hetkellä ne koettiin puutteellisiksi. Työkalu koettiin ”oikein toimivaksi” ja toinen tekijöistä koki, että ”työkalu herättää miettimään, miten asioihin kannattaa varautua. Ei anna suoraan vastauksia, vaan herättää hyvin kysymyksiä!” Tarinat saivat myös kiitosta.

8.4 Yhteenveto koekäyttäjien kokemuksista

Työkalua koekäyttäneistä organisaatioista missään ei ollut laadittu kirjallisia ohjeita tai suunnitelmia tietoturvallisuusasioista. Kaikissa organisaatioissa paljastui jonkinlaisia puutteita ja käytäntöjä, joita olisi hyvä korjata. Erityisesti koekäyttäjä A:n yrityksessä huomattiin, että tietoturvallisuustilanne on aivan retuperällä. B ja C saivat työkalusta lisää kimmoketta jo suunnitelmatasolla olevan tietoturvallisuustyön suuntaamiseen ja kehittämiseen, ja A:n toimitusjohtaja heräsi niihin riskeihin, joita yritystoiminnassa ei ollut aikaisemmin ajateltu. Koekäytön tulokset työkalusta ovat lupaavia, ja vastaavat sitä, mitä työkalulla tavoiteltiinkin. Kaikissa organisaatioissa työkalu todettiin hyödylliseksi ja ajatuksia herättäväksi, ja kaikki koekäyttäjät kertoivat ryhtyvänsä käytännön toimiin työkalun osoittamien puutteiden korjaamiseksi. Työkalua korjattiin B:n antaman palautteen mukaisesti parempaan muotoon sekä sisältönsä että ulkoasunsa puolesta.

9 Johtopäätökset ja oman työn arviointi

Koostin yhteenvedon työkalun koekäyttäjiltä saamastani ja korjasin työkalua sen pohjalta. Muun muassa työkalun ulkoasu sai perusteltua palautetta, joten luovuin ”Mitä oikein tapahtui?”-osion kömpelöstä nelikentästä ja korvasin sen neljällä, allekkain olevalla tekstilaatikol-

la. Lihavoin tekstilaatikoista avainsanoja lukijan katseen ohjaamiseksi, jotta työn nopeallakin silmäilyllä laatikoista löytää olennaiset sanat.

Työn tekemisen ja tiedonhankinnan yhteydessä keskeiseksi johtopäätökseksi nousi se, että tietoturvallisuustietoisuuden lisääminen on tärkein askel pienten yritysten tietoturvallisuustilanteen kohentamisessa. Tämän tietoisuuden lisäämisessä käytännön esimerkkeihin nojaava työkalu on hyvä tapa konkretisoida muuten hieman abstrakteina näyttäytyviä riskejä. Pääsääntöisesti yrityksissä halutaan hoitaa asiat hyvin, mutta tietoturvallisuuteen liittyvät kysymykset ovat vaikeita ja koetaan lähinnä vaikeina, teknisinä haasteina. Tietoturvallisuustilanteen kuntoon saattamiseen on käytettävissä koekäyttövastausten perusteella pienissä yrityksissä varsin vähän resursseja. Koska kyse on kuitenkin yritysten perustason riskienhallinnasta, on tietoturvallisuuden vaikeaa lähestyttävyyttä hälvennettävä ja yrittäjiä on ohjattava heidän osaamistasolleen sopivien tietolähteiden piiriin. Tekemällä edes hieman perustyötä tietoturvallisuusasioidensa parissa saavutetaan jo hyviä tuloksia. Paras tulos saavutetaan, kun tietoturvallisuuskäytännöt otetaan huomioon jo yrityksen toiminnan käynnistämisvaiheessa, jolloin jo olemassa olevia käytäntöjä ei tarvitse lähteä muuttamaan.

Tietämättömyys tietoturva-asioista tuntuu johtuvan usein myös välinpitämättömyydestä niitä kohtaan. Molemmat teemat linkittyvät toisiinsa siten, että yhdistyessään tietämättömyys ja välinpitämättömyys muodostavat toisiaan vahvistavan asenneparin, jossa koulutusta ja tietoa ei haeta, koska sitä ei mielletä tarpeelliseksi. Koska tietoa ja koulutusta tietoturvallisuudesta ei ole, sen hankkimista ei pidetä tärkeänä. Tämä johtaa tilanteeseen, jossa tietoturvallisuustyö yrityksissä on laiminlyöty. Kyselyn perusteella myös mobiililaitteiden tietoturvallisuus edellyttää runsaasti työtä yrityksissä, jotta niitä koskevat tietoturvallisuusseikat saadaan kuntoon. Vauhdilla yleistyneiden älypuhelinten ja tablettien tieturvahaasteet ovat yrityksille nopeasti ratkaisuja kaipaava osa-alue.

Teemoittelun perusteella hahmotettu tilanne näkyy työkalussa siten, että tarinoissa on pyritty tuomaan esille tilanteita, joita olisi voitu välttää, mikäli tietoturvallisuusasiat olisi otettu huomioon yritystoiminnassa ja ne miellettäisiin tärkeiksi. Tarinat on rakennettu siten, että niiden esittämät riskit olisi voitu välttää kohentamalla tietämättömyydestä ja välinpitämättömyydestä johtuvia asioita.

Opinnäytetyön tekemisen suurimmaksi haasteeksi nousi kyselylomakkeiden huono vastausprosentti, sillä toivoin saavani laajemman skaalan vastauksiini joista voin laskea tarkempia keskiarvoja valtakunnan tietotekniikkarikostutkijoiden näkemyksistä. Sain kuitenkin vain viidenneksen lähettämistäni lomakkeista takaisin, mutta niiden varsin yhtenäinen sisältö loi kuitenkin luottamusta siihen, että teemoittelemalla vastaukset voidaan löytää yleisiä asioita, joiden perusteella työkalun sisältöä voidaan kohdentaa.

Kyselytutkimuksen heikosta vastausprosentista huolimatta siinä saadut vastaukset tukivat omiin havaintoihini perustuvaa käsitystä siitä, että tietoturvallisuutta pienissä yrityksissä uhkaa pääsääntöisesti tiedon puute. Tietoturvallisuuden eri osa-alueiden hahmottaminen ei ole itsestään selvää, kuten työkalun koekäytössäkin kävi ilmi.

Koekäyttö antoi lupaavia tuloksia työkalun rakenteesta ja siinä tehdyistä tyylillisistä valinnoista, ja työkalu tuntui toimivan juuri siten, miten sen oli tarkoituskin toimia. Koekäyttäjät kokivat sen hyödylliseksi nimenomaan tarinapohjaisen rakenteen vuoksi. Tietoturvallisuuden lähestyminen sen ongelmien kautta oli hyvä tapa ”herättää” työkalun käyttäjä tiedostamaan niitä moninaisia riskejä, joita tietoturvallisuuden laiminlyönti voi yrityksessä aiheuttaa.

Lähteet

Andreasson, A. & Koivisto, J. 2013. Tietoturvaa toteuttamassa. Helsinki: Tietosanoma.

Andrews, D., Hull, T. & Donahue, J. 2009. Storytelling as an Instructional Method: Descriptions and Research Questions. Viitattu 31.1.2014. http://www.au.af.mil/au/awc/awcgate/afrl/storytelling_instructional.pdf

Doty, E. 2003. Transforming Capabilities: Using Story for Knowledge Discovery & Community Development. Viitattu 31.1.2014. http://www.worklore.com/WorkLore_TransformingCapabilities_EDoty.pdf

Hakala, M., Vainio, M. & Vuorinen O. 2006. Tietoturvallisuuden käsikirja. Helsinki: Docendo.

Helsingin Sanomat. 2014. Kyberrikollisuus ylittää jo huumekaupan. Viitattu 13.1.2014. http://www.hs.fi/ulkomaat/Kyberrikollisuus+ylitt%C3%A4%C3%A4+jo+huumekaupan/a1389234680993

Kirchgaessner, S. 2013. Cloud storage carries potent security risk. Financial Times. Viitattu 31.1.2014. http://www.ft.com/cms/s/0/4729ed7c-3722-11e3-9603-00144feab7de.html#axzz2ryOATHR3

KvantiMOTV – Kvantitatiivisten menetelmien tietovarasto. 2010. Kyselylomakkeen laatiminen. Viitattu 30.1.2014. http://www.fsd.uta.fi/menetelmaopetus/kyselylomake/laatiminen.html

KvantiMOTV – Kvantitatiivisten menetelmien tietovarasto. 2007. Mittaaminen: muuttujien ominaisuudet. Viitattu 30.1.2014 http://www.fsd.uta.fi/menetelmaopetus/mittaaminen/ominaisuudet.html#likert

Laaksonen, M., Nevasalo, T. & Tomula, K. 2006. Yrityksen tietoturvakäsikirja. Helsinki: Edita.

Lagus, A. 2013. Entä jos meille murtaudutaan? Tietosuoja-lehti 4/1023. 26-28.

Layton, T. 2007. Information security design, implementation, measurement and compliance. Boca Raton: Auerbach Publications.

Plain Language at Work. 2012. Plain Language at Work Newsletter 25.2.2012. Viitattu 31.1.2014. http://www.impact-information.com/impactinfo/newsletter/plwork51.htm

Puolustusministeriö. Kansallinen turvallisuusauditointikriteeristö KATAKRI II. 2011. Viitattu 19.1.2011. http://www.defmin.fi/files/1525/KATAKRI.pdf

Saaranen-Kauppinen, A. & Puusniekka, A. 2006. KvaliMOTV - Menetelmäopetuksen tietovaranto. Viitattu 29.1.2014. http://www.fsd.uta.fi/menetelmaopetus/

SFS-ISO 31000. 2011. Riskienhallinta. Periaatteet ja ohjeet. Helsinki: Suomen standardoimisliitto.

Silius, K. 2008. Teemoittelu ja tyypittely-kalvosarja. Tampereen teknillinen yliopisto. Viitattu 31.1.2014. http://matriisi.ee.tut.fi/hmopetus/hmjatkoopintosemma/2008/Silius_teemoittelu-tyypittely_141108.pdf

Taanila, A. 2013. Otantamenetelmä. Viitattu 30.1.2014. http://tilastoapu.wordpress.com/2012/03/09/otantamenetelma/

Taloussanomat. 2014. Taloussanakirja. Viitattu 19.1.2014. http://www.taloussanomat.fi/porssi/sanakirja

Tietosuojavaltuutettu. 2013. Ota oppaaksi henkilötietolaki! Viitattu 30.1.2014. http://www.tietosuoja.fi/uploads/wvzmhnffsvyrhb5.pdf

Tiivis tietoturvasanasto. 2004. Sanastokeskus TSK. Viitattu 19.1.2011. http://www.tsk.fi/fi/info/TiivisTietoturvasanasto.pdf

Tilastokeskus. 2014. Käsitteet ja määritelmät. Viitattu 12.1.2014 http://www.stat.fi/meta/kas/pk_yritys.html

Uusi Suomi. 2014. Opisto mokasi: ”Poista sähköposti avaamatta”. Viitattu 5.2.2014. http://www.uusisuomi.fi/kotimaa/65591-virasto-mokasi-poista-sahkoposti-avaamatta

Valtionvarainministeriö. 2008. Valtionhallinnon tietoturvasanasto. VAHTI 8/2008. Viitattu 31.1.2014. https://www.vahtiohje.fi/web/guest/348

Valtionvarainministeriö. 2011. Johdon tietoturvaopas. . VAHTI 2/2011. Viitattu 14.9.2013. http://www.hare.vn.fi/mJulKaisujenSelailu.asp?h_iId=12914&ju_iId=4690

Viestintävirasto. 2014. Kyberturvallisuuskeskuksen ohjeet. Viitattu 18.1.2014. https://www.kyberturvallisuuskeskus.fi/ohjeet.html

Viestintävirasto. 2013. Tietoturvaopas. Viitattu 12.9.2013. http://www.tietoturvaopas.fi

Vilkka, H. & Airaksinen, T. 2003. Toiminnallinen opinnäytetyö. Helsinki: Tammi.

Volonino, L. & Anzaldua, R. 2008. Computer forensics for dummies. Hoboken, NJ: Wiley publishing.

Kuviot

Taulukot

Liitteet

Liite 1 Asiantuntijakyselyn kysymyslomake

Vastaa joko lomakkeelle tai sähköisesti antti.kurittu@gmail.com, otsikoksi ”opinnäytetyökysely”.

1. Missä tehtävissä työskentelet?

   _____

2. Käsitteletkö työssäsi pienten ja keskisuurten yritysten tietoturvallisuusasioita?

   _____

3. Käsitteletkö työssäsi **rikosasioita** ja jos kyllä, niin missä roolissa (alleviivaa)?

   Kyllä / En asianomistajan edustaja / viranomainen / todistaja / asiantuntija

4. Mitkä ovat mielestäsi yritysten keskeiset **käytännöt** jotka altistavat tietoturvaloukkauksille?

   _____

5. Mitkä ovat mielestäsi yritysten keskeiset **politiikat** jotka altistavat tietoturvaloukkauksille?

   _____

6. Miten seuraavat asiat ovat **oman arviosi** mukaan **keskimäärin** yrityksissä, joiden asioita käsittelet? Anna arvosana yhdestä viiteen jossa 1 = toteutettu erittäin huonosti 5 = toteutettu erittäin hyvin.

a. Tietoturvallisuusohjeistus	1	2	3	4	5
b. Tietoturvallisuuskoulutus	1	2	3	4	5
c. Tietoturvallisuustietoisuus	1	2	3	4	5
d. Toimitilaturvallisuus	1	2	3	4	5
e. Varmuuskopiointi ja datan säilyttäminen	1	2	3	4	5
f. Mobiililaitteiden tietoturvallisuus	1	2	3	4	5
g. Salasanahallinta	1	2	3	4	5
h. Tietojen ja dokumenttien turvallisuusluokittelu	1	2	3	4	5
i. Paperitulosteiden käsittely	1	2	3	4	5
j. Tietoverkkoturvallisuus	1	2	3	4	5

   Listaa kolme yleisintä asiaa, käytäntöä tai politiikkaa jotka altistavat yrityksen tietoturvaloukkauksille:

   1. _____
   2. _____
   3. _____

   Taustatietoja vastaajasta

   Sukupuoli: M / N Ikä: _____ Työkokemus: _____

TIKKA

-

Tietoturvallisuustilanteen kartoitustyökalu pienille yrityksille

Versio 1.1

Helsinki

antti.kurittu@gmail.com

Tervetuloa käyttämään pienten yritysten tietoturvallisuustilanteen kartoitustyökalua Tikkaa!

Tikka-kartoitustyökalu on suunniteltu sellaisten yritysten tarpeisiin, joissa tietoturvallisuustyö on kokonaan tekemättä, joissa sitä aletaan vasta suunnitella tai jossa sen toteuttaminen on vielä alkuvaiheessa. Jokaisella yrityksellä, niin pienellä kuin suurellakin, on suojaamisen arvoista tietoa, vaikka tiedonkäsittely ei olisikaan yrityksen päätoimialaa.

Tämä työkalu kertoo kuusi fiktiivistä tarinaa, joiden laatimisessa on käytetty hyväksi muun muassa yksityiskohtia tosielämän tietotekniikkarikostapauksista ja muista tietoturvaa uhkaavista onnettomuuksista.

Tarinat liittyvät tietoturvallisuuden eri osa-alueisiin – hallinnolliseen turvallisuuteen, fyysiseen turvallisuuteen, henkilöstöturvallisuuteen, tietoaineistoturvallisuuteen, ohjelmistoturvallisuuteen ja laitteistoturvallisuuteen. Joissakin tarinoissa yhdistyy elementtejä useammasta tietoturvallisuuden osa-alueesta.

Toimivan tietoturvallisuuden ylläpitäminen yrityksessä on osa yrityksen perustason riskienhallintaa. Tietoturvallinen toiminta perustuu selkeisiin periaatteisiin, joita noudattamalla yritys voi suojautua yleisimmiltä tietoturvaa uhkaavilta tapahtumilta.

Tietoturvaloukkaukset ovat yrityksen tiedolliseen pääomaan kohdistuvia riskitekijöitä. Tietoturvaloukkaukset voidaan jaotella sisäisiin ja ulkoisiin loukkauksiin, joiden erona voidaan pitää tietoturvaa uhkaavan tapahtuman alkupistettä. Myös vahingot ja onnettomuudet ovat tietoturvauhkia. Tässä työkalussa esiintyvissä tarinoissa on tapauksia molemmista kategorioista.

Tee työkalu lukemalla tarinat ajatuksella läpi. Lue tämän jälkeen seuraavalta sivulta tarinaan liittyvät vinkit ja neuvot. Aseta tarinassa tapahtuvat asiat oman yrityksesi kontekstiin ja kysy itseltäsi jokaisen tarinan lopussa olevat kolme kysymystä oman yrityksesi tietoturvallisuudesta. Olennainen, koko työkalun kantavana teemana oleva kysymys on *”voisiko näin tapahtua minun yrityksessäni? Olemmeko ottaneet huomioon tällaisen tilanteen?”*

Jos työkalun käyttämisen jälkeen olet tunnistanut omassa yritystoiminnassasi olevia tietoturvariskejä ja päättänyt ryhtyä niiden suhteen käytännön toimiin, on työkalu toiminut tarkoituksensa mukaan.

Työkalun päätehtävä on lisätä tietoisuutta niistä mahdollisista tapahtumista ja seurauksista, joita huonosti hoidettu tietoturvallisuus voi aiheuttaa. Tarinan muotoon kirjoitetut skenaariokuvaukset on valittu työkalun sisällöksi siksi, että ne tuovat riskit ja niiden seuraukset lähelle arkielämää.

Tietoisuus riskeistä ja niistä mahdollisesti seuraavista vahingoista on ensimmäinen askel oman yrityksen tietoturvatalkoissa.

Riskien hallinta on aina helpompaa kuin vahingoista toipuminen!

1 Myyntipäällikköä huijataan

Pentti työskentelee myyntipäällikkönä yrityksessä. Hän vastaa työtehtävissään asiakkaille laadittavien tarjousten laatimisesta. Pentillä on luonnollisesti pääsy yrityksen sisäverkkoon myös kotoaan, sillä hän matkustaa työnsä puolesta paljon ja tietoturvaohjeiden mukaan yrityksen tietoja saa tallentaa vain sisäverkkoon. Pääsy yrityksen sisäverkkoon on varmistettu käyttäjätunnuksella ja salasanalla, joka pitää vaihtaa kolmen kuukauden välein. Pentti pitää aina mukanaan yrityksen konetta, jonka kovalevy on salakirjoitettu. Tietoturvan pitäisi siis olla teknisesti kunnossa.

Yritys on ulkoistanut ylläpito- ja IT-tukipalvelut ja siirtänyt yrityksessä ennen IT-tukena toimineet henkilöt toisiin tehtäviin. Tällä tavoin yritys on säästänyt rahaa ja pystynyt keskittymään omaan ydinosaamisalueeseensa.

Pentti on työmatkalla Ikaalisissa kun hän saa työsähköpostiinsa viestin IT-tuelta. Viestissä kerrotaan, että Pentin toimistolla sijaitsevalle työasemalle on tullut internetistä virus, ja IT-tukihenkilön tulisi kirjautua etäyhteydellä työasemalle virustorjuntaohjelman ajamista varten. Virustorjunnan ajamista varten Pentin pitäisi kirjautua verkkoon sähköpostissa annetusta linkistä.

Sähköposti on tullut IT-tuen sähköpostiosoitteesta ja siinä on oikean yrityksen logo. Viestikin on kirjoitettu siistillä ja selkeällä suomenkielellä. Pentti klikkaa sähköpostissa olevaa linkkiä ja syöttää sieltä aukeavalle verkkosivulle käyttäjätunnuksensa ja salasanansa.

Pentti pelkää, että työasemalle tuleva virus voi aiheuttaa vahinkoja, joten hän ei aikaile toimenpiteen suorittamisessa. Sivusto antaa kuitenkin virheilmoituksen, ja Pentti sulkee sen.

Hetken kulutta Pentti saa toisen sähköpostin jossa kerrotaan, että virustorjunta onnistuttiin suorittamaan virheestä huolimatta, ja ettei Pentin tarvitse enää huolia asiasta.

Muutamaa viikkoa myöhemmin käy ilmi, että kilpaileva yritys on voittanut tärkeän tarjouskilpailun yllättävän pienellä marginaalilla. Pentin yrityksessä uskottiin, ettei kilpailija pysty tuottamaan palvelua heitä halvemmalla ja tulisi häviämään kilpailun.

Asiaa selvittämään palkattu tieturva-asiantuntija huomaa toimiston lähiverkon lokitiedoista, että Pentin käyttäjätunnuksella on kirjauduttu Maltalle johtavasta IP -osoitteesta yrityksen verkkoon ja ladattu kaikki tiedostot, mitä Pentin käytössä olevalta verkkolevyltä löytyi.

Yrityksen yhteisellä verkkolevyllä oli paljon myös sellaisia dokumentteja, joita Pentti ei tarvitse työssään, mutta yrityksessä on ollut tapana, että kaikki tieto tallennetaan samalle verkkolevylle, mihin kaikilla on vapaa pääsy. Vahingot hävitystä kilpailusta nousevat lopulta kymmeniin tuhansiin euroihin.

Mitä tarinassa tapahtui?

Pentti joutui **kohdennetun tietojenkalastelun** uhriksi. Tietojen kalastelu, eli niin sanottu ”phishing” on tietoturvahyökkäys, jossa hyökkääjä erehdyttää uhriaan antamaan tälle käyttäjätunnuksen, salasanan tai muita tärkeitä tietoja joiden avulla suojauksia voidaan murtaa. **Kohdennettu tietojenkalastelu**, ”spear phishing”, käyttää hyväkseen yksityiskohtaisia tietoja uhrista, kuten tämän kotiosoitetta, saadakseen urkinnan näyttämään uskottavammalta.

Kyse on ensisijaisesti **hallinnollisen turvallisuuden** ongelmasta, sillä ainoa keino torjua tietojenkalastelu on riittävä koulutus sen tunnistamiseksi. Etätyöskentelyä varten tehdyt tekniset suojaukset ovat hyödyttömiä, jos uhri luovuttaa itse kirjautumistunnuksensa hyökkääjälle. Kohdennettu tietojenkalastelu voi olla erittäin uskottavaa, eikä uhri välttämättä huomaa tulleensa huijatuksi, eikä tieto tapahtuneesta koskaan tule ilmi.

Henkilöstön on syytä tietää, että **henkilökohtaista salasanaa ei saa luovuttaa kenellekään** missään olosuhteissa. Ylläpito voi suorittaa kaikki toimenpiteensä saamatta salasanaa tietoonsa. Ulkoistettujen IT-tukipalveluiden käyttö johtaa siihen, ettei IT-tukihenkilö ole työntekijälle tuttu joten hyökkääjän on helppo esiintyä tällaisena. Kaikkiin tietokyselyihin pitää suhtautua varovaisesti.

Työntekijät tulee kouluttaa tunnistamaan tietojenkalasteluhyökkäykset ja varmistamaan kaikki epäilyttävät viestit esimerkiksi puhelimitse IT-tukipalveluilta tai omalta esimieheltään. Salasanan on pysyttävä salaisena. Tietokoneisiin liittyviin tukitoimintoihin on hyvä olla olemassa selkeä prosessi, jotta poikkeukselliset yhteydenotot erottuvat.

Kolme kysymystä oman yrityksesi tietoturvasta

1. Onko yrityksesi henkilökunta koulutettu tunnistamaan ja raportoimaan tietojenkalasteluyritykset esimiehelleen tai tietohallinnolle?

2. Tietävätkö työntekijät, että IT-tuki ei kysy koskaan käyttäjien salasanoja eikä pyydä heitä kirjautumaan puolestaan järjestelmiin?

3. Onko etätyöhön käytettävä yhteys suojattu esim. VPN-salauksella tai muilla teknisillä ratkaisuilla?

2 Murtovarkaat toimistolla

Insinööritoimisto Mynttinen & Pesonen on perustanut konttorinsa Helsingin Töölöön, katutasoon. Kaverukset ovat löytäneet valoisat tilat vanhasta, kauniista rakennuksesta ja päässeet toteuttamaan omaa sisustussilmäänsä tilojen suunnittelussa. Toimistossa on isot, kauniit ikkunat jotka antavat pienelle tilalle suuren toimiston tuntua.

Työ sujuu hyvin ja asiakkaita riittää taantumasta huolimatta. Mynttinen ja Pesonen asuvat kumpikin lähistöllä ja nauttivat siitä, että voivat joka päivä kävellä kauniin Helsingin katuja pitkin työpaikalleen.

Toimisto sijaitsee sivukadulla poissa pahimmasta kaupungin melskeestä, jolloin työrauhakin säilyy.

Eräänä yönä Mynttisen puhelin soi ja ruudulla näkyy outo numero. Vartioimisliikkeen hälytyskeskuksen päivystäjä soittaa kertoakseen, että toimistolta on aamuyöstä tullut lasirikkohälytys. Vartija on ehtinyt paikalle viidessätoista minuutissa hälytyksen vastaanottamisesta, mutta oli paikalle saavuttuaan vain todennut ammottavan reiän toimiston etuoven lasissa.

Paikalle kutsutaan poliisi, ja Mynttinen rientää itsekin kotoaan tarkistamaan tuhoja. Poliisi tekee alueella lähietsintöjä, mutta ei kuitenkaan hyvistä yrityksistä huolimatta enää löydä pakoon pötkineitä murtoveikkoja. Tiloissa ei ollut kameravalvontaa, joten tekijöistä ei saatu edes kuvaa.

Tiloja tarkistaessaan Mynttinen huomaa, että varkaille on kelvannut ainakin uusi videotykki, kahvihuoneen kolikkopurkki, Mynttisen pöydällä ollut avonainen tupakka-aski, pöydällä lojunut ulkoinen kovalevy sekä kaksi kannettavaa tietokonetta Mynttisen ja Pesosen työpöydiltä. Tietokoneilla oli Mynttisen ja Pesosen työtiedostoja, perheen valokuvia, sähköpostikirjeenvaihtoa kolmen vuoden ajalta ja iso liuta Mynttisen omia, henkilökohtaisia tiedostoja.

Ajantasaisia varmuuskopioitakaan ei ollut olemassa, koska varmuuskopiointia hoidettiin epäsäännöllisesti ulkoiselle levylle, jota säilytettiin toimistolla. Senkin varkaat veivät. Osa tiedostoista oli tallessa sähköpostissa ja Mynttisen entisellä koneella, osa taas katosi pysyvästi varkaiden matkaan.

Mynttinen palaa kotiin pää painuksissa ja kaivaa komerosta vanhan tietokoneensa. Aamulla olisi edessä soitto asiakkaalle, että ensi viikoksi sovittua suunnittelupalaveria olisi lykättävä, ja projekti myöhästyisi.

Mynttisellä oli edessään monta unetonta yötä kun jo kertaalleen tehdyt työt piti tehdä uusiksi. Lisäksi Mynttistä vaivasi tietokoneella olevat intiimit valokuvat, joita he olivat vaimonsa kanssa ottaneet muutaman viinilasillisen jälkeen. Etteivät nyt vaan päätyisi internetiin…

Mitä tarinassa tapahtui?

Mynttinen & Pesonen joutuivat aivan tavallisen **liikemurron** uhriksi. Vaikutukset kohdistuivat ensisijaisesti omaisuuteen, mutta omaisuuden mukana varastettiin myös arvokasta tietoaineistoa. Toimiston murtosuojaus oli puutteellinen ja sen lisäksi isoista ikkunoista oli selkeästi nähtävillä arvokasta, varkaita houkuttavaa omaisuutta.

Kyseessä on ensisijaisesti **fyysiseen turvallisuuteen** liittyvä ongelma. Toimistotilat sijaitsivat katutasossa ja niihin pääsi sisälle ikkunan rikkomalla. Syrjäinen sijainti sivukadulla antoi Mynttisen ja Pesosen lisäksi myös varkaille työrauhan. Arvokas omaisuus oli helposti ja nopeasti anastettavissa eikä hälytinkään pelottanut vikkeliä varkaita.

Liiketilojen murtosuojauksessa tulee huomioida omaisuuden menetyksen lisäksi **myös tiedon menetyksen mahdollisuus**. Tärkeä tieto on kahdennettava myös sen varalta, että tietoa sisällään pitävät laitteet **varastetaan** tai **tuhotaan**. Paikallinen verkkotallennuslevy voidaan sijoittaa sellaiseen paikkaan, josta sitä ei ulkopuolinen helposti löydä.

Näkyvyys katutason liiketiloihin on hyvä rajata esimerkiksi verhoilla tai vaihtoehtoisesti maitokalvoilla, jolloin valo pääsee sisään. Ikkunoiden murtolujuutta voi lisätä turvakalvoilla tai panssarilasilla. **Helposti anastettava arvo-omaisuus on syytä kiinnittää paikalleen** tai ainakin nostaa pois näkyvistä kun tiloissa ei oleskella. Kannettavat tietokoneet tulee salakirjoittaa siten, ettei tietoja saa auki ilman salasanaa.

Kolme kysymystä oman yrityksesi tietoturvasta

1. Onko yrityksesi tiloihin asennettu hälytyslaitteet, valvontakamerat, murtosuojauskalvot tai turvalukot?

2. Onko yrityksesi toimipaikalla säilytettävä omaisuus kiinnitetty rakenteisiin ja mahdollisuuksien mukaan poissa ulkopuolisten silmistä?

3. Onko yrityksessäsi tietoa, joka menetetään, jos yksittäinen tietokone varastetaan tai tuhoutuu?

3 Vakoilija sähköpostilaatikossa

Tuomas työskentelee toimitusjohtajana pienessä yrityksessä, joka tuottaa ja suunnittelee pienyritysten toimistokalusteratkaisuja. Tuomas on perustanut yrityksen osakeyhtiönä lapsuudenystävänsä Henrin ja tämän vaimon Riitan kanssa. Yrityksessä on kolmikon lisäksi kuusi vakituista työntekijää, jotka tekevät pääsääntöisesti myyntityötä.

Tuomaksen ja yhtiökumppaneiden välit ovat kuitenkin tulehtuneet viime aikoina yrityksen toimintaan liittyviin erimielisyyksiin, ja tämän lisäksi Henri epäilee, että Tuomaksella on silmäpeliä Riitan kanssa.

Riidat eivät ratkea, joten kolmikko sopii yhdessä, että Henri ja Riitta ostavat Tuomaksen ulos yrityksestä lunastamalla Tuomaksen osakkeet. Osakekauppa sujuu ongelmitta ja Tuomas vaihtaa maisemaa.

Tuomas saa työpaikan kilpailevasta yrityksestä ja etenee nopeasti esimiesasemaan. Kiireessään päästä Tuomaksesta eroon ei huomattu laatia kilpailukieltosopimusta, mutta Henri ja Riitta olettavat, ettei Tuomas kuitenkaan kehtaisi käyttää hyväkseen entisen yrityksen asiakastietoja.

Henri ja Riitta huomaavat kuitenkin pian, että asiakkaita alkaa kadota Tuomaksen uudelle työnantajayritykselle. Tuomas tuntuu olevan muutenkin yllättävän hyvin perillä siitä, mitä Henrin ja Riitan yrityksessä tapahtuu.

Eräänä päivänä yrityksen asiakaspalveluun käytettävästä sähköpostilaatikosta katoaa viestejä, ja Riitan epäilykset heräävät. Tuomas vei töissä käyttämänsä tietokoneen mukanaan, sillä se oli hänen omansa. Lukeeko Tuomas vielä yrityksen sähköposteja?

Asiasta tehdään rikosilmoitus, ja rikostutkinnassa selviää, että Tuomas on tosiaankin lukenut edelleen kaikki viestit, joita yrityksen sähköpostilaatikkoon tulee. Ollessaan vielä perustamassaan yrityksessä töissä Tuomas oli vastuussa työntekijöiden sähköpostilaatikoiden, ja niiden salasanojen, luomisesta.

Henri oli vaihtanut asiakaspalvelun sähköpostilaatikon salasanan, mutta oli tiedottanut uuden salasanan kaikille työntekijöille sähköpostitse. Kaikki työntekijät eivät olleet vaihtaneet Tuomaksen heille antamia salasanoja omiin sähköpostilaatikkoihinsa, joten Tuomas pystyi kirjautumaan tietokoneeltaan erään työntekijän sähköpostiin. Sieltä Tuomas oli saanut tietoonsa asiakaspalveluun käytettävän sähköpostilaatikon salasanan, ja oli pystynyt seuraamaan kilpailijansa sähköposteja uudelta työpaikaltaan omalla tietokoneellaan monen kuukauden ajan.

Tuomas jäi kiinni vasta poistettuaan vahingossa viestejä laatikosta, jolloin rikos huomattiin.

Mitä tarinassa tapahtui?

Tuomaksella oli hallussaan yrityksen toimintaan käytettävä tietokone, ja siellä oli tallessa yrityksen vanhaa sähköpostikirjeenvaihtoa. Lisäksi Tuomaksen luomia salasanoja ei vaihdettu, **koska kukaan ei tullut ajatelleeksi**, että niitä olisi syytä vaihtaa. Asiakaspalvelusähköpostiin pystyi kirjautumaan internetistä eikä kirjautumislokeja seurattu.

Kyseessä on niin **henkilöstöturvallisuuden** kuin **tietoaineistoturvallisuudenkin** ongelma. Yrityksellä ei ollut olemassa ohjeistusta siitä, miten uusien työntekijöiden salasanat luodaan ja miten poistuvien työntekijöiden pääsy tileille estetään. Lisäksi asiakaspalvelusähköpostiin oli pääsy kaikkialta. Oliko tämä tarpeen? Työthän tehtiin aina toimistolla.

Salasanojen luomisen jälkeen **jokaisen käyttäjän on vaihdettava ne yksilöllisiin, vain itse tietämiinsä salasanoihin**. Uudet salasanat yhteisiin resursseihin pitää jakaa sellaisella tavalla, etteivät ne leviä muiden tietoon. Tällaiset salasanat voidaan kirjata esimerkiksi muistioon, jota säilytetään kassakaapissa.

Yrityksen tulee laatia **selkeät ohjeet** siitä, miten tietoaineistojen turvallisuus varmistetaan irtisanoutumistilanteessa. Vanhat tilit tulee poistaa käytöstä siten, että niillä olevat yrityksen tiedot saadaan haltuun. **Omien laitteiden käyttöä työpaikalla tulee rajoittaa** eikä niitä saa käyttää työhön liittyvän materiaalin tallentamiseen.

Kolme kysymystä oman yrityksesi tietoturvasta

1. Onko yrityksselläsi selkeät, kirjalliset ohjeet käyttäjien ja ylläpitäjien salasanojen hallitsemiselle?

2. Onko yrityksselläsi kirjallinen toimintasuunnitelma niin aloittavien kuin poistuvienkin työntekijöiden varalta?

3. Vaihdetaanko toiminnan kannalta keskeisten tietojärjestelmien salasanat määräajoin?

4 Potilastiedot verkossa

Sakari perustaa kotisairaanhoitopalveluita tarjoavan yrityksen yhdessä sairaanhoitajavaimonsa kanssa. Sakari on pitkän linjan yrittäjä, ja kaipaa elämäänsä uusia haasteita.

Uuden yrityksen liiketoiminta lähtee kasvamaan nopeasti ja pian yrityksellä onkin 34 työntekijää. Sakari on tyytyväinen. Suurin osa asiakkaista tulee yritykselle kaupungin sosiaalitoimen kautta, ja maksu hoidetaan maksusitoumuksen avulla.

Sakari vie eräänä päivänä kotiin vanhan kannettavan tietokoneensa, jota hän on käyttänyt töissään. Hän kuitenkin haluaa käyttöönsä uudemman mallin ja antaa vanhan tietokoneensa 12-vuotiaalle pojalleen. Poika on kiinnostunut tietokoneista, ja Sakari katsookin tyytyväisenä poikansa harrastusta. Ehkä poika joskus työllistyisi arvostetulle IT-alalle.

Poika formatoi tietokoneen kovalevyn ja asentaa siihen käyttöjärjestelmän. Sakari palauttaa varmuuskopioista uudelle tietokoneelleen vanhat työtiedostonsa, jotka on asianmukaisesti varmuuskopioitu toimiston verkkolevylle.

Eräänä päivänä poika tulee kuitenkin itku silmässä kotiin ja kertoo hukanneensa uuden tietokoneensa. Poika oli jättänyt tietokoneen koulussa käytävälle reppuun, josta se oli oppitunnin aikana varastettu. Sakari lohduttelee poikaansa, ja myöhemmin samana päivänä he käyvät ostamassa pojalle uuden koneen kadonneen tilalle. Muutaman viikon päästä poliisista otetaan yhteyttä Sakariin kuulustelukutsun merkeissä. Asema on ”rikoksesta epäilty”. Sakari on hämmentynyt, mistä häntä nyt epäillään?

Kuulusteluissa poliisi kertoo löytäneensä internetistä listan sadoista potilaista, joiden kaikkien yhteinen nimittäjä on se, että he olivat Sakarin asiakkaita. Listalla oli potilaiden yksityisiä terveystietoja - kaikki taudinkuvauksista henkilötunnuksiin ja osoitteisiin asti. Tiedoilla oli tehty jo muun muassa petoksia ja otettu pikavippejä potilaiden nimiin. Sakaria epäillään ainakin henkilörekisteririkoksesta.

Myöhemmin selviää, että henkilörekisterin muodostavat potilastiedot oli palautettu pojalta varastetun tietokoneen kovalevyltä ja laitettu rikollisten toimesta verkkoon. Teon motiivi jää epäselväksi.

Tietokoneen pojan laukusta varastanut koulun oppilas oli myynyt koneen verkossa eteenpäin muutamalla kympillä. Tietokoneen ostanut rikollinen oli kokeillut ilmaiseksi saatavia tiedonpalautustyökaluja ja huomannut, että koneen levy oli tyhjennetty puutteellisesti. Suurin osa tiedostoista oli vielä palautettavissa.

Sakarin huolimaton toiminta johti siihen, että sosiaalitoimi purki yrityksen kanssa solmimansa sopimuksen ja yritystoiminta kärsi valtavan tappion.

Mitä tarinassa tapahtui?

Sakarin yrityksessä oli **laiminlyöty** henkilötietojen käsittelyyn liittyvä **huolellisuus**. Käytettävien laitteiden elinkaarta ei oltu ajateltu yrityksen tarpeita pidemmälle, eikä tietojen **turvallisen poistamisen** merkitystä oltu ymmärretty. Sakari oli myös siinä uskossa, että formatointi tyhjentää levyn niin, ettei tietoja voi enää palauttaa.

Kyseessä on **tietoaineistoturvallisuuden** ongelma. Tietokoneella olevat tiedostot eivät poistu levyn formatoinnin yhteydessä, vaan tallennusväline pitää joko päällekirjoittaa tai tuhota lukukelvottomaksi. Kaikki laitteet, joilla arkaluontoista tietoa käsitellään, pitää poistaa käytöstä tietoturvallisilla menetelmillä.

Laitteet, joilla käsitellään arkaluontoisia tietoja, tulee merkitä selkeästi ja niitä ei pidä tarpeettomasti kuljettaa yrityksen tiloista pois. Laitteiden jälleenmyynti-, kierrätys- tai edelleenluovutustilanteissa tallennusmediat tulee **poistaa ja tuhota** tai ylikirjoittaa. Sama koskee ulkoisia tallennusvälineitä kuten USB-tikkuja tai irtokovalevyjä. Myös kopiokoneet tallentavat usein kopioitavia dokumentteja kovalevyilleen.

Käsiteltävät tiedot on syytä luokitella esimerkiksi neljään eri luokkaan julkisiksi, sisäisiksi, luottamuksellisiksi ja salaisiksi. Tietojen käsittelyohjeissa on otettava huomioon tietojen **koko elinkaari** niiden luomisesta niiden tuhoamiseen. Julkisten tietojen poistamisessa ei tarvitse olla erityisen tarkkana, mutta salaisten tiedostojen poistaminen edellyttää huolellisuutta ja tietoturvallisia toimintatapoja.

Kolme kysymystä oman yrityksesi tietoturvasta

1. Onko tallennusvälineistänne laadittu elinkaarisuunnitelma, joka ottaa huomioon välineille tallennetun aineiston turvallisen hävittämisen?

2. Onko salassa pidettävät tiedot selkeästi erotettu julkisista tai sisäisistä tiedoista, joiden erityinen suojaaminen ei ole tarpeen?

3. Jos yrityksessäsi käsitellään henkilötietoja, onko niistä muodostuvasta henkilörekisteristä laadittu rekisteriseloste?

5 Päivittämättömät laitteet

Automaatiosuunnittelualan yritys on toiminut kohta vuosikymmenen toimitusjohtaja Matin ja uskollisen miehistön voimin. Yritys tekee tasaisen varmaa tulosta, ja työtä tuntuu tulevan samaa tahtia kuin sitä saadaan valmiiksi. Yrityksen operaatiot toimivat rutiinilla, ja muutamista yritystoimintaa uhkaavista riskeistä on toivuttu hyvän jatkuvuussuunnittelun ja sinnikkään yritysjohdon ansiosta.

Yrityksen perustamisvaiheessa hankittiin koneellista piirtämistä varten tietokoneita, jotka korvasivat käsin tehtävän suunnittelutyön. Työntekijätkin olivat saaneet koulutuksen ohjelmistoon ja työ sujui sillä hyvin. Työasemiin kului rahaa, mutta suurin investointi oli ohjelmiston lisenssi, joka maksoi 15 000 euroa ja sisälsi viiden vuoden ylläpitosopimuksen.

Ylläpitosopimusta jatkettiin vielä kahdella vuodella, mutta ohjelmistoyhtiö ilmoitti, että yrityksen käyttämää versiota ei enää jatkossa tueta sillä se perustuu vanhaan ohjelmistoarkkitehtuuriin. Vanhana asiakkaana Matille tarjottiin uuden ohjelmiston lisenssiä kolmenkymmenen prosentin alennuksella hintaan 10 000 euroa. Hintaan sisältyi ylläpitosopimus.

Samassa yhteydessä olisi pitänyt uusia laitteet ja niihin kuuluvat käyttöjärjestelmät, mutta Matti katsoi, että työt sujuvat vanhallakin ohjelmistolla joten päivitykseen ei ollut tarvetta. Kului muutama vuosi ja työt sujuivat hyvin, kunnes eräänä päivänä toimiston kaikki tietokoneet olivat lukossa. Kukaan toimistolla ei saanut yhtäkään konetta auki, ja mystiset virheilmoitukset eivät auttaneet asiassa laisinkaan.

Matin yritys kääntyi tietoturva-asiantuntijapalveluita tarjoavan yrityksen puoleen, ja yritykseltä tuli paikan päälle asiantuntija tarkistamaan tilanteen.

Vanhoihin laitteisiin ei enää oltu julkaistu tietoturvahaavoittuvuuksia korjaavia päivityksiä. Eräs yrityksen työntekijä oli saanut verkkosivuilta koneelleen viruksen, joka levisi koko sisäverkossa kaikkiin koneisiin. Suunnitteluohjelman sisäinen tietoliikenneprotokolla oli avannut lähiverkosta ulkoverkkoon reitin, jota pitkin virus pääsi koneeseen. Ohjelma tarvitsi tätä reittiä tiedonsiirtoon muiden koneiden kanssa, mutta siitä hiljattain löydetty haavoittuvuus oli jäänyt paikkaamatta toimittajan siirryttyä tukemaan uutta versiota.

Virus lukitsi koneet ja pyyhki niiltä järjestelmätiedostoja. Matin ei auttanut muu kuin sammuttaa kaikki laitteet ja lähettää ne huoltoon. Samalla oli marssittava tietokoneliikkeeseen hankkimaan uusia laitteita ja ohjelmistolisenssiä.

Uusien laitteiden asennuksen ajan työt seisoivat ja työtiedostojen palauttaminen varmuuskopioilta vei kaksi viikkoa. Kun uudet laitteet saatiin käyttöön, huomattiin, että uusi versio ohjelmasta oli nopeampi, ja siinä oli paljon ominaisuuksia, joita edelliseen versioon oli pitkään kaivattu.

Mitä tarinassa tapahtui?

Matin yrityksessä laiminlyötiin **ajantasaisten ohjelmistojen** käyttäminen ja uskottiin vanhojen olevan käyttökelpoisia vielä pitkään. Vanhoista ohjelmistoista löytyy usein **tietoturva-aukkoja**, eikä ohjelmistontoimittajilla ole usein resursseja tai halua paikata vanhoja versioita samalla tarkkuudella kuin uusia. Tämä altistaa vanhat ohjelmat haavoittuvuuksille ja väärinkäytöksille.

Kyseessä on **ohjelmistoturvallisuuden** ongelma. Matin olisi pitänyt laatia ohjelmistoille päivityssuunnitelma ja uusia laitteistonsa ajantasaiseksi hallitusti. Verkon selailu työntekoon tarkoitetuilla työasemilla pitää estää ja sitä varten voidaan hankkia oma kone. Verkon turvallisuuteen liittyvät ohjelmat kuten tietokoneiden käyttöjärjestelmät ja virustorjunta on pidettävä ajan tasalla.

Ohjelmistojen toimittajien kanssa on käytävä läpi uusien ja vanhojen versioiden erot ja laadittava suunnitelma isommille versiopäivityksille. **Lisenssienhallintaan** liittyy myös riittävien ylläpito- ja tukipalveluiden hankkiminen. Tukipalvelut huolehtivat päivitysten jakelemisesta ohjelmistojen loppukäyttäjille.

Tietotekniset laitteet eivät ole ikuisia. Sama koskee myös ohjelmistoja. Niiden elinkaari mitataan muutamissa vuosissa. Erityisesti raskaat teollisuusohjelmistot edellyttävät tietokoneilta paljon tehoa, ja investoimalla riittäviin ja ajantasaisiin työkaluihin myös työn tulokset – ja turvallisuus – pysyvät laadukkaina.

Kolme kysymystä oman yrityksesi tietoturvasta

1. Onko toimintanne kannalta olennaisten laitteiden ohjelmisto- ja laitetuki sovittu palveluntuottajan kanssa?

2. Ovatko työtehtävien hoitamisen kannalta kriittiset työasemat yhdistetty internetiin?

3. Ovatko laitteidenne turvallisuusohjelmistot ja –asetukset ajantasaisia?

6 Suunnittelijan laiterikko

Sani on perustanut yrityksen, joka tuo maahan ja tuottaa omaan mallistoonsa laukkuja, kodintekstiilejä, sisustus- ja muotituotteita. Tavaraa on sekä omasta mallistosta että hyvin tunnettujen ulkomaalaisten tuottajien katalogeista.

Hän on aloittanut liiketoiminnan kotoaan ompeluhuoneestaan sivutoimena, mutta ahkeruutensa ja lahjakkuutensa johdosta yrityksen liiketoiminta on kasvanut joka vuosi huimasti. Pian Sani siirtyy toimistotiloihin Helsingin keskustaan ja palkkaa avukseen varastonhoitajan, toisen suunnittelijan sekä myyntimiehen. Liiketoiminnan keskipiste siirtyy omaan mallistoon, joka myy hyvin ja saa kehuja maailmalla.

Sani tekee suunnittelutyön pääasiassa omalla tietokoneellaan ja käyttää paljon sähköpostia sekä sosiaalista mediaa viestintään.

Yrityksen menestyessä sähköistä materiaalia alkaa kertyä niin paljon, että sen jakaminen työntekijöiden kesken käy vaivalloiseksi. Sani käy ostamassa elektroniikkaliikkeestä ulkoisen kovalevyn, jonka saa kytkettyä yrityksen lähiverkkoon. Hän vertailee hintoja, ja päätyy noin 200 euron hintaiseen laitteeseen.

Sanin ystävä käy asentamassa levyn ja verkottaa työntekijöiden tietokoneet niin, että kaikilla on omilta tietokoneiltaan pääsy uudelle verkkolevylle. Nyt kaikki tieto saadaan kätevästi jaettua toimiston väen kesken ja työ sujuu helpommin.

Eräänä aamuna Sani saapuu työpaikalleen ja käynnistää tietokoneensa. Verkkolevy-yhteys ei kuitenkaan käynnisty, eikä hän saa avattua uuden käsilaukkumalliston suunnittelutiedostoja. Kukaan toimistolla ei osaa korjata levyjärjestelmää, joten Sani soittaa ystävälleen joka tulee tarkistamaan sen toiminnan.

Ystävän tarkistaessa levyä käy ilmi, että yöllä raivonnut ukkosmyrsky on antanut sähköverkon ylitse jännitepiikin, joka on tuhonnut ulkoisen kovalevyn täysin. Tietojen palauttaminen levyltä edellyttäisi levyn lähettämistä asiantuntijayritykselle, jonka korjausarvio liikkuu tuhansissa euroissa, mikäli tiedot on ylipäänsä mahdollista palauttaa.

Kylmä hiki kohoaa Sanin otsalle kun hän muistaa, että uuden malliston suunnittelutiedostot ovat vain verkkolevyllä. Omalla koneellaan hän ei niitä säilytä, sillä hän pelkää, että kone varastetaan.

Sani joutuu aloittamaan kuukausia hiomansa työn alusta ja menettää samalla entisten projektiensa tiedostot, tärkeitä yhteystietoja sekä muita tiedostoja joita levylle oli tallennettu.

Sani ottaa yhteyttä asiantuntijaan, joka suosittelee Sanille varmuuskopioivaa verkkotallennuslevyä sekä pilvipalvelua, johon tiedot varmistetaan automaattisesti. Ratkaisu maksaa alle tuhat euroa, ja tiedot ovat jatkossa tallessa.

Mitä tarinassa tapahtui?

Levyrikko on tietoturvallisuuden kannalta ongelma. Levylle taltioitu tieto on fyysisesti levyn pinnalla, ja jos yrityksessä luotetaan siihen, etteivät laitteet koskaan vikaannu, on tietoturva retuperällä. Pahimmassa tapauksessa tietojen menetys voi johtaa liiketoiminnan loppumiseen. Tiedonpalautus hajonneilta levyiltä ei aina onnistu, ja onnistuessaankin se on kallista.

Kyseessä on sekä **fyysisen turvallisuuden** että **laitteistoturvallisuuden** ongelma. Fyysinen turvallisuus voidaan varmistaa suojaamalla toiminnan kannalta kriittiset laitteet ulkoisilta häiriöiltä. Tietoaineistoturvallisuus voidaan varmistaa varautumalla laitteiden vikaantumiseen varmuuskopioimalla tärkeät tiedot. Vikasietoiset laitteet ovat kalliimpia, mutta halvempia kuin vahingosta aiheutuvat kulut.

Kaikki yrityksen toiminnan kannalta tärkeä tieto pitää **vähintään kahdentaa** paikallisesti eri levyille, ja mieluiten varmuuskopioida fyysisesti eri paikkaan, esimerkiksi pilvipalveluun tai toiseen toimipaikkaan. Sähköverkon virranjakelun häiriöiltä voi suojautua käyttämällä siihen suunniteltuja laitteita. Vikasietoisten laitteiden käyttö on käytännössä **yhtä helppoa** kuin helposti vikaantuvienkin.

Käytä kaikkia tiedontallennusratkaisuja miettiessäsi hieman vaivaa siihen, että hankit vikasietoisia laitteita ja seuraat aktiivisesti niiden toimintaa. Häiriöiden ennakoiminen säästää aikaa, vaivaa ja rahaa pitkällä aikavälillä. Aloituskustannukset ovat suuremmat, mutta kokonaiskustannukset matalammat. Yrityksen toiminnan kannalta tärkeää tietoa ei saa koskaan säilyttää **vain yhdessä paikassa.**

Kolme kysymystä oman yrityksesi tietoturvasta.

1. Onko yrityksesi kaikki tärkeä tieto varmuuskopioitu ajantasaisesti?

2. Ovatko tallennus- ja tietojärjestelmänne suojattu sähkönjakeluverkon häiriöiltä?

3. Onko kaikki tieto keskitetty verkkolevylle, vai säilytetäänkö työasemilla tärkeitä tietoja?

Saatteeksi

Olet nyt tehnyt Tikka-kartoitustyökalun loppuun. Toivottavasti nämä tosielämään perustuvat esimerkkitarinat valaisivat, millaisista käytännön asioista puhutaan, kun puhutaan tietoturvallisuuden hallinnasta.

Kyse on lopulta arkisista riskeistä, joiden hallitseminen ei edellytä valtavaa teknistä osaamista tai vaikeiden, teknisten ratkaisujen hallitsemista.

Yrityksen toimiva tietoturvallisuuskulttuuri lähtee yrityksen toiminnan määrittelemästä, tarkoituksenmukaisesta suunnittelusta, suunnitelman tarkasta toteutuksesta ja jatkuvasta havainnoinnista.

Joidenkin tietoturvallisuuden osa-alueiden kuntoon saattamisessa kannattaa turvautua luotettavan asiantuntijan apuun. Tärkeintä on kuitenkin aloittaa tietoturvallisuustyö nyt, ennen kuin vahinko ehtii tapahtua.

Riskien torjuminen on aina parempi vaihtoehto kuin jälkien korjaaminen!

Onnea ja menestystä yrityksesi tietoturvatalkoisiin!

Antti Kurittu | antti.kurittu@gmail.com

Lisätietoja pienyrityksen tietoturvallisuuden hallinnasta saat Viestintäviraston tietoturvaoppaasta osoitteesta

www.tietoturvaopas.fi.

Ajantasaista tietoa suomalaisia yksityishenkilöitä ja yrityksiä uhkaavista tietoturvauhista saat Viestintäviraston Kyberturvallisuuskeskuksen sivuilta osoitteesta

www.kyberturvallisuuskeskus.fi.

Henkilötietojen käsittelyä koskevia ohjeita saat tietosuojavaltuutetun toimiston verkkosivuilta osoitteesta

www.tietosuoja.fi.

Valtionvarainministeriön VAHTI-ohjeet ovat yksi maailman kattavimmista yleisistä tietoturvaohjeistoista. Vapaasti saatavilla olevat VAHTI-ohjeet voit katsoa osoitteesta

www.vahtiohje.fi.

Puolustusministeriön kansallisen turvallisuusauditointikriteeristön KATAKRI II:n ohjeet löydät osoitteessa

www.defmin.fi/